Governance, Risk, and Compliance Handbook

Technology, Finance, Environmental, and International Guidance and Best Practices

Edited By

Anthony Tarantino, PhD

John Wiley & Sons, Inc.

Additional Praises for *Governance, Risk, and Compliance Handbook*

"In just a few short years, GRC has quickly risen to become a top boardroom and management priority at leading organizations around the world. And with business and regulatory environments becoming increasingly complex, the corporate-wide focus on GRC shows no sign of slowing down. The GRC Handbook is a comprehensive guide to the key strategies, tools and best practices that can help companies build and manage a proactive, integrated, cross-enterprise GRC strategy. For companies large or small, across all industries and geographies–this thorough study approaches GRC from multiple perspectives and is a must-have resource for any manager tasked with aligning GRC activities to drive business performance and competitive advantage."

—Jim Hagemann Snabe, Corporate Officer SAP Group, Member of the Executive Council

"This book provides insightful views of the challenges and lessons learned from the implementation of International and US standards in Latin America. Highly recommended for anyone interested in Global Compliance."

—Zenon A. Biagosch, Certified Fraud Examiner, Member of the Board of Directors, Central Bank of Argentina

"The GRC Handbook is a must-read for all those involved in Global Compliance. The new international landscape and the interaction among laws, regulations, and professional standards are comprehensively covered in this book."

—Dr. Francisco J. D'Albora Jr., Certified Fraud Examiner, JD. Designated Crime Prevention Expert for the Organization of the American States. Co-judge of the Federal Criminal Justice of Argentina. President of the Argentina Foundation against Money Laundering and Financing of Terrorism.

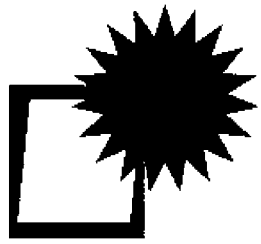
"Dr. Anthony Tarantino has produced a classic reference volume on governance, risk, and compliance. His book provides a comprehensive overview of current practices across the globe. This book is a must for practitioners, risk managers, and senior executives."

—June Yee Felix, General Manager, General Manager Global Banking Solutions and Strategy, IBM

"Today, global level governance, risk management, and compliance are strong management tool for successful international companies. Leading players in this area gain their competitive advantage by penetrating their management style to their every regional entity. Governance, Risk, and Compliance Handbook is unique and comprehensive because it not only covers key GRC topics but also explains governance by industry and by nation. The text will be a good guide for executives and managers who involve in global management."

—Satoshi Arai, Leader of Risk, Compliance & Security, Japan Management Director, BearingPoint Co., Ltd.

Governance, Risk, and Compliance Handbook



Subscriber Update Service

BECOME A SUBSCRIBER!

Did you purchase this product from a bookstore?

If you did, it's important for you to become a subscriber. John Wiley & Sons, Inc. may publish, on a periodic basis, supplements and new editions to reflect the latest changes in the subject matter that you ***need to know*** in order to stay competitive in this ever-changing industry. By contacting the Wiley office nearest you, you'll receive any current update at no additional charge. In addition, you'll receive future updates and revised or related volumes on a 30-day examination review.

If you purchased this product directly from John Wiley & Sons, Inc., we have already recorded your subscription for this update service.

To become a subscriber, please call **1-800-225-5945** or send your name, company name (if applicable), address, and the title of the product to:

mailing address: **Supplement Department**
John Wiley & Sons, Inc.
One Wiley Drive
Somerset, NJ 08875

e-mail: **subscriber@wiley.com**
fax: **1-732-302-2300**

For customers outside the United States, please contact the Wiley office nearest you:

Professional & Reference Division
John Wiley & Sons Canada, Ltd.
22 Worcester Road
Rexdale, Ontario M9W 1L1
CANADA
(416) 675-3580
Phone: 1-800-567-4797
Fax: 1-800-565-6802
canada@jwiley.com

John Wiley & Sons, Ltd.
Baffins Lane
Chichester
West Sussex, PO19 1UD
ENGLAND
Phone: (44) 1243 779777
Fax: (44) 1243 770638
cs-books@wiley.co.uk

Jacaranda Wiley Ltd.
PRT Division
P.O. Box 174
North Ryde, NSW 2113
AUSTRALIA
Phone: (02) 805-1100
Fax: (02) 805-1597
headoffice@jacwiley.com.au

John Wiley & Sons (SEA) Pte. Ltd.
2 Clementi Loop #02-01
SINGAPORE 129809
Phone: 65 463 2400
Fax: 65 463 4605; 65 463 4604
wiley@singnet.com.sg

Governance, Risk, and Compliance Handbook

Technology, Finance, Environmental, and International Guidance and Best Practices

Edited By

Anthony Tarantino, PhD

John Wiley & Sons, Inc.

This book is printed on acid-free paper. ♾

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Governance, risk and compliance handbook : technology, finance, environmental and international guidance and best practices / edited by Anthony Tarantino.

p. cm.

Includes index.

ISBN 978-0-470-09589-8 (cloth)

1. Corporate governance. 2. Risk management. 3. Compliance auditing. I. Tarantino, Anthony, 1949-

HD2741.G695 2008

658.15′1–dc22

2007038100

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

To my Beloved Xuelian

"Everyone must submit himself to the governing authorities, for there is no authority except that which God has established. The authorities that exist have been established by God. Consequently, He who rebels against the authority is rebelling against what God has instituted, and those who do so will bring judgment on themselves. For rulers hold no terror for those who do right, but for those who do wrong. Do you want to be free from fear of the one in authority? Then do what is right and he will commend you. For he is God's servant to do you good. But if you do wrong, be afraid, for he does not bear the sword for nothing. He is god's servant, an agent of wrath to bring punishment on the wrongdoer. Therefore, it is necessary to submit to the authorities, not only because of possible punishment but also because of conscience. This is also why you pay taxes, for the authorities are god's servants, who give their full time to governing. Give everyone what you owe him: if you owe taxes, pay taxes; if revenue, then revenue; if respect, then respect; if honor, then honor.

Romans 13: 1-7: Submission to the Authorities

The Mandate of Heaven is conditioned on virtuous rule, is not perpetual or automatic and depends on good governance worthy of a virtuous sovereign. The Mandate of Heaven can be lost through the immoral behavior of the ruler, or failings in his responsibility for the welfare of the people, in which case Heaven will grant another, more moral individual a new mandate to found a new dynasty. Loyalty will inspire loyalty. Betrayal will beget betrayal. A king unworthy of his subjects will be rejected by them. Such is the will of Heaven.

Mencius (Meng-Tze), 孟子, Book of Mencius, (371-288 B.C.)

CONTENTS

URL CONTENTS

Supplemental material for the Handbook can be accessed online at www.wiley.com/go/grchandbook

PREFACE

My first book, The Manager's Guide to Compliance, was released in April 2006, and provides an introduction to internal controls over risks required to meet financial and technical regulations. While it provided overviews to international standards and regulations, the coverage was limited and did not include country, environmental, or industry-specific guidance. It also became apparent that compliance was part of a triad that must encompass both governance and risk.

The inspiration to write a second book came a little over a year ago when we received the news that the first book was to be translated into Chinese, demonstrating a growing global interest in compliance and risk-related issues. The Governance, Risk, and Compliance (GRC) Handbook is designed to greatly expand the coverage provided in the first book. GRC is now a widely accepted approach that has at its core a holistic approach to governance, risk, and compliance. The reason to treat GRC in a holistic manner is simply that to attack them separately is a costly mistake, causing duplicated efforts and greater chances of failure in all three areas.

The text is designed to be a true handbook in the sense that it provides very wide coverage, but at a higher and introductory level. It includes detailed country and regional guidance for the major economies of the world, guidance for several industries, guidance for national and regional environments, technology tools guidance, operational risk guidance, and more in-depth corporate governance guidance. The goal of each chapter is to provide an introduction to the subject and point the reader to sources for a more detailed discussion. In short, to provide truly global coverage.

Typical of most handbooks, each chapter is designed to stand on its own and not require the reader to review the entire text to understand a given topic. The combined print and URL content spans over 1,000 pages, with sixty-five contributors, While GRC is a very dynamic area, the handbook covers the major trends and trusts and should be seen as a valuable resource for the coming years.

Like all successful handbooks, the plan is to provide periodic updates and supplements as conditions warrant. Your comments and suggestions will be most welcome to guide the future direction of this work. This can include authoring additional chapters or suggested resources for any of the topics covered. My contact information is provided below for this reason.

For this edition, we reached out to over 600 resources. Our 64 contributors have become a community of GRC advocates and were very helpful in bringing

in a wide variety of subject matter experts and providing guidance as to additional content. The one bias we all share is the belief that improved GRC is in everyone's best interest and will grow in importance as the globe continues to shrink.

Anthony Tarantino
December 2007
agtarantino@hotmail.com

ACKNOWLEDGMENTS

I would like to acknowledge the consistent support and encouragement of my editor at John Wiley & Sons, Timothy Burgard, to our great editorial coordinator, Helen Cho, our terrific production editor, Lisa Vuoncino, and to our index editor, Shirley Cui Tarantino.

I would also acknowledge the amazing collaboration and support of the 64 contributors from 15 countries to this effort. Not only did they work tirelessly to provide leading-edge content, but they were also able to enlist other colleagues to contribute and review.

ABOUT THE CONTRIBUTORS

Hélen de Aguiar is Brazilian and an executive for the biotechnology affairs, and an economist with specialization in public services costs and environmental management. She is currently president of the "Sindicato Estadual das Empresas de Biotecnologia do Estado de Minas Gerais" (Environmental Union for the State of Minas Gerais) and a member of the State of Minas Gerais Industry Federation. She co-sourced with over 200 projects in environmental management and social and economical development across Brazilian territory, including Bioremediation of Aurá (a project that was awarded with "best practices" prize by ONU in 2000 and 2004). Helen also represents the State of Minas Gerais in the Special Committee for environmental-related subjects of the Environmental Ministry and is the coordinator of the export project involving biotechnological-based companies from 2003 thru 2005. She is the author of *Brazilian Biotechnology, Business Opportunity and Competitive Advantage*.

Sanjay Anand, CFE, CCD, is a globally recognized expert on corporate governance and regulatory compliance, with about 20 years of deep experience as a strategic advisor, certified consultant, professional speaker, and published author in business process management, project risk management, business and technology audits, and enterprise technologies. His clients include over a hundred companies, many of them Fortune 500 and Global 2000 companies, from over a dozen industries from around the globe. He is the recipient of such awards as the J. D. Edwards Consultant of the Year, Northeast Area Special Achievement, Global Enterprise Solutions Outstanding Performance, and Client Services Valuable Teamwork.

Koti Ancha has had over 16 years of experience in manufacturing operations, supply chain management, and systems integration and consulting. He is a certified six sigma black belt and a certified Lean Master. He currently works for Seagate Technology in the supply chain group, where six sigma and lean methodologies are embraced and extensively used to gain competitive advantage in the marketplace.

C. L. Bansal has a Masters degree in Economics and is associated with Management Development Institute (MDI), Gurgaon, India for more than three decades. He has been the Dean of MDI for seven years (1996–2003) and head of the executive MBA program for three years (1993–1996) besides being the Editor of Management Journal of MDI (1989–1999). Professor Baxi teaches Economics and Corporate Governance subjects at the post graduate courses and also designs and delivers executive development programs.

He has been a visiting Fellow at the JL Kellogg Graduate School of USA (1993) and the Australian National University Canberra Australia (2000). He has

also conducted training programs on behalf of the ADB and the World Bank for the South Asian financial institutions. He has published two books on Corporate Governance and one on Corporate Social Responsibility (sponsored by the UNDP, CII, and AICTE). Since 2003 Professor Baxi is the Chairman of Corporate Governance Center MDI, Gurgaon, India.

Dr. C. V. Baxi is presently a Professor of Law at MDI, Gurgaon, India. He has over three decades of academic experience in various reputed institutions in India. He is currently heading the law faculty at MDI. He holds an LLB from Delhi University, Diploma in Administrative Law, Indian Law Institute, besides being a Fellow Member of the Institute of Company Secretaries of India. He holds a Doctorate in the area of Corporate Governance from Delhi School Economics. He has to his credit publications in the area of Corporate Governance. He has been a consultant with the Institute of Company Secretaries and All India Management Association.

Francesca Bevilacqua was born in Ravenna in 1975. In 2001 she obtained a degree in business administration at Bocconi University, Milan. She then joined the audit firm PricewaterhouseCoopers as auditor. After achieving experience in business analysis, in 2004 she decided to continue her career in the executive search consultancy. She joined Hunters Strategic Executive Search as a researcher and after a year joined Governance Consulting as research manager of the search business unit. Governance Consulting is an integrated professional skills firm focused on corporate governance issues; its services include executive search, management appraisal, and compensation systems, as well as the development of suitable solutions for the adoption of codes of ethics and professional training programs aimed at effectively implementing the adopted governance systems.

Alan Calder is a leading author and speaker on the issues of data security and IT governance and an advisor to companies including Cisco. He has led training, consultancy, and industrial services companies in Europe and North America. He led the world's first successful BS7799 implementation. He was a member of DTI's Information Age Competitiveness Working Group and is a member of the DNV Certification Services Certification Committee, which certifies compliance with international standards, including ISO 27001. IT Governance Ltd (ITGL) is a leading global authority on data security and IT governance for business and the public sector. It is the world's most comprehensive publisher of and distributor for information, advice, guidance, books, and tools for governance, risk management, and compliance.

L. Nelson Carvalho holds both a Master and a PhD degree from University of São Paulo (Brazil), where he teaches both at the undergraduate and graduate levels. He researches on Corporate Governance, Auditing and Risk Management, and International Accounting. Nelson was appointed in July 2005 to serve as the first independent Chairman of the Standards Advisory Council of the International Accounting Standards Board until December 2008. He is a litigation expert both in Brazil and abroad, on Capital Markets, Financial Accounting, and Auditing.

Nelson has served as the Head of Banking Supervision of the Central Bank of Brazil and also as a Commissioner of the Brazilian SEC.

Oneglia Andrade Cavalcanti is a Local Manager with Control Solutions International, in the Brazil office, who has a diverse background in risk management, distribution, quality, manufacturing, and internal audit. At Control Solutions, she worked with the following clients: CA, COOPER-STANDARD, GEMPLUS, ICI QUEST, UNIFI DO BRASIL and ALCOA among other companies, helping these companies to meet SOX compliance requirements as well as internal audit targets. Prior to joining Control Solutions, she was a partner in O&N SERVIÇOS. Previous engagements with O&N SERVIÇOS also included implementation of quality management systems, auditing for ISO 9001:2000 compliance, and training. While with XEROX, she also held positions as six sigma (Black Belt), Cost Down Analyst, Export Control Analyst, and Quality Supervisor.

Deborah Cernauskas, PhD is currently a risk management consultant for IBM. Her career includes time spent in both academia and industry. She has taught finance at both the graduate and undergraduate levels at several Chicago-area universities, including Northern Illinois University. Her industry experience is multifaceted, including experience in corporate development, operational finance, market research, and commodities trading research. Her research is currently focused on hedging operational risks and using Bayesian estimation methods in value at risk (VAR) and portfolio allocation decisions.

Massimiliano Claps is a program manager in the public sector within IDC's European Vertical Markets Group. In this position he analyzes and anticipates key trends and forecasts on IT strategies and spending in central and local government, health care, and education in Western Europe. Claps' research looks into the structure and composition of national government organizations by major agency types, the dynamics of public budgets and procurement, and their impact on IT spending, as well as the impact of the regulatory framework and of the European Commission's eEurope initiatives on IT deployment levels. Claps' contribution also extends to public-sector-specific events presentations, as well as articles in several government- or IT-specific magazines; his opinions and insights on IT strategies in government and the public sector are quoted also in world-renowned newspapers, such as the *International Herald Tribune* and the *Financial Time*s. Prior to joining IDC, Claps developed extensive marketing studies and competitive analysis expertise working as a consultant with the Monitor Company, where he participated in several projects for large Italian and multinational firms. He obtained a degree in business administration from Bocconi University in Milan.

Harald Collet is a first lieutenant and platoon commander in the Danish Army and holds a bachelor of arts degree with distinction from Yale University. As the Senior Director of Governance, Risk, and Compliance (GRC) Solutions for Oracle Corporation, Harald is responsible for global go-to-market programs,

solution sales, and product strategy. He manages a global team of solution specialists in Europe and North America who work with strategic customers to unlock global GRC challenges. While at Oracle, Harald was also a principal product manager for content management products and a group marketing manager in Oracle's marketing organization. Prior to joining Oracle in 2001, Harald spearheaded the competitive intelligence program at Internet Appliance Network, a New York–based technology firm working with major companies to create branded hardware and marketing services.

Dennis Cox is CEO of Risk Reward Limited, a strategy and risk consultancy for the financial services industry, as well as being a CEO or director of a number of other companies. He was formerly director of risk management at HSBC Operational Risk Consultancy and global risk director at Prudential Portfolio Managers Limited, having spent 12 years in practice with Arthur Young and BDO Binder Hamlyn. He is a fellow of the Institute of Chartered Accountants in England and Wales (ICAEW) and also of the Securities and Investments Institute (SII). Among a range of external interests he is a senior council member of the ICAEW and a member of the Professional Standards Board, together with being chairman of the Risk Forum for the SII. He also represents the public interest in the regulation of the Institute of Actuaries for financial service matters.

Michael F. Cox is a procurement compliance manager for a Silicon Valley Fortune 500 test and measurement equipment manufacturer. He is also pursuing a graduate degree in supply management leadership. He has managed complex environmental liability cases, and has significant experience in financial, quality, and environmental auditing programs, including acquisition and divestiture due diligence. He has developed and maintains a comprehensive financial, quality, and environmental compliance tool for the firm, including Sarbanes-Oxley Act requirements. He is currently focused on supply chain change management for rapidly evolving electronic product hazardous material restrictions.

Ann Cullen is a business information librarian at Baker Library, Harvard Business School, with a specialty in finance.

Robert G. Eccles is a founder and managing director of Perception Partners, Inc., a company that provides advice and services on corporate governance, corporate reporting, and managing reputational risk. Prior to that he was a tenured professor at Harvard Business School, where he served on the faculty for 14 years. He is the author of two books and many articles on corporate reporting. He is also the lead author of "Reputation and Its Risks" (*Harvard Business Review*, February 2007). Dr. Eccles received an SB in mathematics and an SB in humanities and science from the Massachusetts Institute of Technology and an AM and PhD in sociology from Harvard University.

Frank Edelblut is president and founder of Control Solutions International, the leading provider of independent internal audit, compliance, risk management, and technology solutions. Since 1991, he has guided its rapid growth into a global firm that has delivered services to more than 500 clients in over 35 countries.

He works closely with management in many Fortune 500 companies on internal control and business process improvement, and is an internationally recognized speaker on internal audit and corporate governance. Frank previously spent nine years as an auditor with Price Waterhouse and as CFO of Niagara Corporation, a NASDAQ-listed home therapy equipment manufacturer.

Pedro Fabiano is an international expert with more than 15 years' experience in overseeing internal audit, fraud examination, anti-money laundering, and operational risk. He is a regent emeritus and fellow of the Association of Certified Fraud Examiners (ACFE). He is also former president and co-founder of the Argentina Chapter of the ACFE, the only chapter in Latin America. He has authored the "International Bribery" course published by the ACFE, which is used to train professionals around the world. Most recently, Fabiano has contributed as co-author of the *Fraud Casebook*, edited by Joseph T. Wells.

Angie Fitts, an early trailblazer in Sarbanes-Oxley Compliance, successfully guided Cingular Wireless's compliance program implementation. She continues to drive strategic improvements while navigating a rapidly changing industry, including one of corporate America's largest mergers. For 15 years, she has successfully held manager and director positions in compliance and auditing, specializing in revenue assurance and domestic and international telecommunication operations. Prior to AT&T, Ms. Fitts, a certified public accountant and certified internal auditor, joined Ernst & Young, LLP, after earning her Master of Accountancy in tax from the University of Tennessee. She and her husband, Walt, reside in Atlanta, Georgia.

Joachim Thomas Garson works in business strategy at SAP's High Tech industry unit and oversees partner management for High Tech ISVs, one of them being TechniData. In that role, he established the partner relationship with TechniData for "SAP solution for environmental product compliance," a joint GTM consisting of SAP's Environment, Health, and Safety (EH&S) and TechniData's Compliance for Products (CfP). Thomas and Krishna Gorrepati work closely together in aspects of solution management, partner engagement and joint GTM. Prior to SAP, Thomas worked as consultant at AT Kearney, SAP, and IDS Scheer. Thomas is currently working on a doctoral degree at Tongji University's School of Economics and Management in Shanghai, China.

Saker Ghani is a Senior Consultant with BearingPoints IT Strategy and Architecture practice. A long term proponent of utilizing cutting edge search technology to solve enterprise information access and retrieval problems, Saker was first introduced to the problem of search during his stay at Yahoo!, where he led an engineering team focused on building a world-class content deployment platform for yahoo.com. Saker has since led a number of search architectural projects at North American financial services firms, helping them solve complex compliance and content management challenges. He has also written his own search engine based on the opensource Apache technology, Lucene.

Krishna Gorrepati leads solution management for Compliance for Products (CfP) at TechniData America. As the lead of solution management, Kris guides the development of CfP solutions to address global product environmental regulations such as RoHS, WEEE, REACH, EuP, China RoHS, and others. Kris's prior experience includes founding a successful software company as well as product development and operational roles at Ford Motor Company and Caterpillar. Kris holds a BS and an MS in mechanical engineering and is active in the MBA program at UCLA.

David S. Jacoby, president of Boston Logistics Group (www.bostonlogistics.com), has been consulting to manufacturers, distributors, supply chain software and service providers, and carriers in over a dozen countries for 18 years. He holds an MBA from the Wharton School, a master's in international business from the Lauder Institute, and a BS in economics from the University of Pennsylvania. He is a past president of Boston APICS and the Council of Supply Chain Management Professionals (CSCMP)'s New England Round Table. He also is a director of the Institute for Supply Management (ISM)'s Logistics and Transportation Group, a member of the International Supply Chain Education Alliance (ISCEA)'s Ptak Prize Selection Committee, and a member of the American Society of Transportation and Logistics (AST&L).

Eric Keller is president and CEO of Movaris, Inc., a company that helps finance organizations transform their "last mile" into repeatable, auditable, and efficient processes. He has more than 20 years of experience as a financial executive in high-growth technology companies, and his business background encompasses corporate and international finance, public offerings, acquisitions, intellectual property licensing, and financial information systems. He also has extensive experience in corporate compliance with government agencies.

Michael Kirschner has held the position of president and managing partner of Design Chain Associates, LLC, since its inception in 2001 and is a recognized and oft-quoted expert on the impact of environmental regulation on the electronics industry. Over the previous 20 years he held engineering and engineering management positions at Compaq, Tandem, Intel, and Intergraph, as well as at several start-ups. He received his BSEE from Worcester Polytechnic Institute in Worcester, Massachusetts.

Julia Koo, after getting her MS degree in management science and engineering from Stanford University, joined Oracle USA in 2001. As the principal product strategy manager of Oracle's governance, risk, and compliance (GRC) applications, Julia has been leading this area's product directions, engaging with industry analysts, customers, and prospects, setting partnership strategy, as well as participating in acquisition process and dual diligence projects. Julia has been a speaker at various national and international conferences and events representing Oracle as the compliance domain and product expert. She has also led various internal and external training sessions on Oracle's GRC product offerings.

Richard Kubin is an industry expert in the design, optimization and deployment of cross-enterprise processes and environments for high-tech electronics engineering and manufacturing and is currently Vice President of Solutions Engineering with E2open, a leading provider of solutions for complex supply chain visibility and control. One area of current focus is on product compliance assurance solutions to address the industry requirements of environmental compliance and beyond. Prior to joining E2open, Richard worked for Nortel Networks, where he was most recently the Director of Global Operations Engineering. Richard is the former chair of the IPC 2-18 Supplier Declaration Sub-Committee, which was responsible for the development of the IPC-1752 Material Declaration standard, and is also on the US Technical Advisory Group for IEC TC111, Environmental Standardization for Electrical and Electronic Products and Systems. He is an executive with over fifteen years experience in the software and high tech electronics industry, including 11 years with a Fortune 500 company and four years with a successful software start-up. Richard is also a multiple patent holder with diverse expertise, including semiconductor and telecom product research and development, engineering and business process re-design and implementation, global manufacturing operations, supply chain optimization, and business software development and pre-sales support. Richard has a degree in Mechanical Engineering from the University of Victoria, and also holds 2 US patents in the area of semiconductor packaging.

Lindsey Kudo graduated from the University of Southern California with a bachelor's degree in business administration and a master's in communication management. She then worked for BearingPoint as a consultant assisting in Sarbanes-Oxley readiness, testing, and the implementation of compliance automation software systems. She is currently a controls and compliance manager, assists in running various types of compliance software, and is actively working toward obtaining her CISA certification.

Daniel P. Lawless is a Senior Manager of Compliance Engineering for Broadcom Corporation. His team is responsible for global regulatory approvals of Broadcom's WiFi, Bluetooth, and Gigabit Ethernet products. He is a member of the Executive Committee of the TCB Council. Previously he worked for 3Com and was responsible for global approvals of analog modem, ISDN, and RF products. He has worked as a consultant supporting many of the largest manufacturers of telecom and networking equipment. He has worked in global compliance for more than ten years.

Tim J. Leech is director of corporate trust services with Navigant Consulting in Toronto. Prior to this position he was the principal consultant and chief methodology officer with Paisley Consulting, a leading global provider of business accountability solutions. From 1991 to 2004 he was CEO and founder of CARD®*decisions*, a global pioneer in the ERM and CRSA areas. Other positions he has held include managing director of a subsidiary of the Hambros Bank, director Control & Risk Management Services with Coopers & Lybrand Consulting,

and a range of comptrollership and internal audit roles with Gulf Canada. Tim was elected fellow of the Institute of Chartered Accountants Ontario in 1997 in recognition of distinguished service to the auditing profession. He is the primary author of the IMA discussion paper "A Global Perspective on Assessing Internal Control over Financial Reporting" and author of dozens of articles, presentations, and training modules on SOX, ERM, CRSA, and business ethics.

Lane Leskela is the senior product marketing director for governance, risk, and compliance applications at Oracle Corporation and a recognized IT market specialist on compliance management processes and compliance automation. He is a former research vice president at Gartner, Inc., where he focused on enterprise risk management, regulatory compliance management, and financial controls. Prior to nine years with Gartner, Leskela was an Asia-Pacific financial services industry recruiter for Russell Reynolds Associates in Hong Kong. He served as a program manager for International Data Corporation Asia-Pacific, also based in Hong Kong. In the early 1990s, Leskela was an international trade consultant for China's Jiangxi Province. He earned a bachelor's in international studies and economics from Portland State University and a master's from Columbia University's School of International and Public Affairs in New York. He is a Certified Corporate Finance Consultant.

Wanxin Li is an assistant professor at the School of Public Policy and Management at Tsinghua University, Beijing, China. Her research focuses on regulatory governance and sustainable development. Her dissertation is on how the two pilot environmental performance information disclosure programs impacted environmental regulatory enforcement in China through aligning interests of stakeholders and channeling webs of dialogue among them. Another line of her research is on the institutional capacity of environmental protection agencies. Wanxin Li received her bachelor's degree in precision instruments and her master's in economics from Tsinghua University in 1995 and 2000 respectively. From Virginia Tech, she received her second master's in statistics in 2003 and her PhD in public administration and policy in July 2006.

Luiz Glück Lima is Brazilian, single, and a biologist. He specialized in Tissue Culture and Micropropagation of Tropical Flower, and has a Master's degree in Vegetal Physiology (ongoing).

Luiz Mário Queiroz Lima, EngD is Brazilian, married, a Civil Engineer, and specialized in Thermal Engineer and Fluids. He is a Doctor in Hydraulic Engineering and Sanitation, and has a Post-Doctor's Degree in Environmental Biotechnology and Vegetal Bioengineering. He is the author of the following books: *Remediação de Lixões; Tratamento de Resíduos Sólidos; Combustível do Lixo Urbano;* and *Lixo—Tratamento e Biorremediação*.

Sabah M. Ali Mahmoud is a lawyer of Iraqi origin who was raised in the legal profession with extensive legal experience, having practiced in Civil and Islamic Law (Shariah) Courts in the Middle East. He acts as consultant in Middle East Law and Shariah. He graduated from the Law College in Baghdad in

1958 and obtained the London University Post-graduate Diploma in International Economic Law in 1962. He has practiced in Baghdad and held a variety of posts including (OPEC). In 1977, he established a private practice in Abu Dhabi, UAE in association with British and U.S. law firms and was a joint venture partner in a Dubai practice. During his practice in the UAE until 1991, he advised and represented local and international companies, banks, and clients in a variety of legal matters, including litigation at Civil and Shariah Courts. He now acts as consultant in Middle East law & Shariah based in London with a Regional office in Amman, Jordan. His Baghdad office has also been reactivated.

Michael Mainelli, PhD, FCCA, MSI, originally undertook aerospace and computing research, followed by seven years as a partner in a large international accountancy practice before a spell as corporate development director of Europe's largest R&D organization, the UK's Defense Evaluation and Research Agency, and becoming a director of Z/Yen (Michael_Mainelli@zyen.com). Michael is Mercers' School Memorial Professor of Commerce at Gresham College (www.gresham.ac.uk). Z/Yen is a risk/reward management firm helping organizations make better choices. Z/Yen (www.zyen.com) operates as a think tank that implements strategy, finance, systems, marketing, and intelligence projects in a wide variety of fields, such as developing an award-winning risk/reward prediction engine, helping a global charity win a good governance award, or benchmarking transaction costs across global investment banks. Z/Yen's humorous risk/reward management novel, *Clean Business Cuisine: Now and Z/Yen*, was published in 2000; it was a *Sunday Times* Book of the Week, and *Accountancy Age* described it as "surprisingly funny considering it is written by a couple of accountants."

Richard Marti has over 23 years of global experience in information and business systems spanning a wide range of industries, from Fortune 500 companies to technology start-ups. His specialty is the planning, development, integration, and implementation of solutions, including global risk and compliance, data centers, infrastructure, security, operations, and business processes for enterprises. He has delivered successful engagements in risk and global compliance services (SOX, HIPAA, GLBA, Basel II, AML, Privacy Act); business continuity planning (BCP); disaster recovery (DR); identity management; policy enforcement; information and data security services; network planning, design, and implementation; infrastructure security services (wireless, VoIP, SAN, networks, and applications); and program and project management.

Scott McElhaney is currently a Manager at BearingPoint, Inc., focused on IT compliance, Enterprise Search and Infrastructure Solutions. At BearingPoint, Inc., he led the Enterprise Search Global Education and worked with internal developers, partners, and clients on numerous Enterprise Search initiatives. Scott has led programs as a technical architect for enterprise solutions to many Fortune 500 clients.

Krzysztof Michalak is administrator at the Environment Directorate of the Organization for Economic Cooperation and Development (OECD). As a

specialist in the application of environmental policy instruments, Michalak has been managing OECD-China cooperation in the field of environmental protection. He contributed to several OECD reports on China (including environmental information, governance, water management, and environmental enforcement and compliance). He has coordinated the preparation of the OECD Environmental Performance Review of China to be published in 2007.

Scott L. Mitchell serves as the chairman and CEO of a nonprofit initiative called the Open Compliance and Ethics Group (OCEG). OCEG (www.oceg.org) provides objective standards, guidelines, and online resources to help organizations drive principled performance by integrating governance, risk management and compliance (GRC) processes. Mr. Mitchell is a member of the Committee of Sponsoring Organizations (COSO) Task Force. He has been recognized two years in a row by *Business Finance* magazine as one of the "Top 60 Influencers" in corporate finance, by Treasury & Risk Magazine as one of the "Top 100 Must Influencial People in Finance," and by Human Resource Executive Magazine as one of the top 20 thought leaders regarding the future of human resource management.

Hernan Murdock is director of training and development at Control Solutions International and has over 16 years of experience in education, internal audit, operations, and business analysis. He is a lecturer at Northeastern University in Boston, where for the past five years he has taught management, international business, and ethics. He is the author of articles on internal auditing, whistle-blowing programs, fraud, deception, and behavior profiling and has delivered numerous invited talks and conference presentations at internal audit, academic, and government functions in the United States, Mexico, and the United Kingdom.

Ivano Ortis is program manager for retail, consumer product goods, and transportation-specific research in IDC's Industry Insights team. In his position, Ivano analyzes and anticipates trends in information and communication technology (ICT) and business strategies in select industries in error modes and effects analysis (EMEA) and provides consulting and advisory support to end-user organizations and ICT vendors. Ortis brings over 10 years of experience in ICT and wireless technologies, and he recently increased his focus on radio-frequency identification (RFID), assessing best practices and anticipating investment trends, while delivering keynote presentations at leading events. Prior to joining IDC, Ortis served as business development and marketing manager at a VoIP start-up, worked with Fiat Telematic Services as a program manager, Nokia as a technology sourcing manager, Vodafone as an enterprise sales engineer, Andersen Consulting as a senior analyst, and Harris Semiconductor as an IT consultant.

James G. Robertson, MSc, PE, consultant and principal of Validation Experts LLC, has previously held vice president and engineering management positions. He is a consultant to the pharmaceutical industry on information security, on compliance with FDA regulations, and on SOX Section 404, controls

for IT. He has over 30 years' experience, is named on several patents, has published articles on compliance and engineering subjects, and has served as an expert for 14 legal cases.

Ian Rodgers has over twenty-five years of ERP and strategic business systems implementation experience and has led programs within both the public and private sector including banking, petrochemicals, technology, packaged foods and governmental regulatory agencies. He has worked within a number of Fortune 500 companies as well as high-profile international organizations such as the Bank of England, the London International Stock Exchange and Amsterdam Airport, Schiphol. In addition to these systems implementation roles, Ian has held the position of finance director in the European subsidiary of a Fortune 500 technology company and has presided over the reorganization of the European affiliates of a US technology company. More recently he has overseen the successful deployment of a number of Sarbanes Oxley Act compliance initiatives within the United States with responsibility for the implementation of internal control provisions addressing sections 302, 404, and 409. He is currently a manager and advisor within the Answerthink/Hackett consulting group, a world leader in best practice research, benchmarking, and business transformation services, where he provides strategic business advice as well as guidance in the area of governance, risk, and compliance. Ian Rodgers was formerly a product manager at LogicalApps where he was responsible for the financial reporting controls within the ACTIVE Governance product. He was also Director of Product Management at DBxcel during the inception of the company's continuous audit solution.

Bruno Salotti earned his master's and PhD in accounting from the University of São Paulo. He currently teaches at the School of Economics, Business and Accountancy, University of São Paulo, and is a researcher in corporate governance and capital markets issues. Prior to his teaching career, he worked in the Brazilian capital markets in auditing and accounting firms.

Aparna Sawhney is an associate professor at the Management Development Institute, Gurgaon, India. She is also a research consultant for trade, environment, and World Trade Organization (WTO) issues at the Indian Council for Research in International Economics Relations, New Delhi. Her research interests and publications are in the areas of environmental services, food quality measures, market-based environmental instruments, and WTO negotiation strategies of developing countries. She has written policy and strategy papers for the Indian Ministry of Commerce, ICTSD, TERI, and UNCTAD. Her first book, entitled *A New Face of Environmental Management in India* (Ashgate), was published in 2004.

Tommy Seah is the elected vice chairman of the Association of Certified Fraud Examiners Board of Regents based in Texas. The CFE is a postgraduate professional qualification recognized by the FBI and U.S. Central Intelligence Agency in their recruitment of auditors for combating fraud. His services in providing technical training are much sought after by numerous banks in various

regions, including Germany, Singapore, Malaysia, China, Indonesia, the Philippines, and Taiwan. His previous experience includes systems-based auditing in an American international bank, where he was the senior regional auditor responsible for the bank's audit in the Asia-Pacific region. He has also held the top executive position of chief of internal audit in a prime offshore bank, where his audit duties covered the Singapore and Hong Kong operations of the bank.

Anwar Shah (PhD economics) is the lead economist and program leader for public sector governance at the World Bank Institute, Washington, D.C. He is a member of the executive board of the International Institute of Public Finance, Munich, Germany and also a fellow of the Institute for Public Economics, Alberta, Canada. He has previously served the Canadian Ministry of Finance in Ottawa and the Government of the Province of Alberta, Canada. He pioneered the work on governance indicators at the World Bank and has published extensively on governance issues including an evaluation of the World Bank's governance and anticorruption assistance.

Madeleine Ferris Shaw, CMA, MBA, specializing in international business, is a consultant with over 20 years of global experience in financial analysis and the application of information technology to address common business issues and to develop efficient business processes. She has extensive experience as project manager of cross-functional teams with a mandate to increase operational efficiency and reduce costs. Her industry experience includes oil and gas exploration and production, gas transmission, electrical utilities, manufacturing, and telecommunications. She was a contributor to the book *Sarbanes-Oxley Guide for Finance and Information Technology Professionals*, Second Edition.

Jill Solomon, PhD, is a senior lecturer in finance at Cardiff University, Wales, UK. She holds a PhD in Finance (University of Manchester), a Masters degree in Corporate and International Finance, and a BA (Hons) in Economics. Over the last 10 years, Jill has researched and published extensively in the general area of corporate governance, focusing specifically on corporate governance in South Korea, Taiwan, Saudi Arabia, Japan, and the UK. She has published a best-selling textbook, "Corporate Governance and Accountability" (2007, 2 d edition) which provides a broad coverage of the corporate governance discipline.

Georg Stadtmann is an associate professor at the WHU—Otto Beisheim School of Management in Koblenz, Germany, where he teaches in the department of economics. His main research interests lie within the areas of international finance. He has published in the fields of market efficiency, central bank intervention, and expectation formation processes in financial markets. He is also a lecturer at the Leon Kozminski Academy of Entrepreneurship and Management in Warsaw, Poland. In his rare spare time, he fishes at the Rhine River and tries to catch the fish of his life.

Mark Stebelton, CPA, has been involved in the compliance and regulatory field for over 15 years. With a background in public accounting, leading financial and internal audits, Mark has more recently been focused on developing software

that addresses the application governance arena as a senior product manager for LogicalApps, Inc.

Carole S. Switzer, Esq., is President of the nonprofit Open Compliance and Ethics Group (OCEG) (www.oceg.org), which provides objective guidelines and resources to help organizations Drive Principled Performance™ by integrating governance, risk management, and compliance (GRC) processes. Ms. Switzer leads OCEG's work with GRC experts to develop specific guidelines and standards for policies, personnel structures, training and evaluation of GRC systems. Ms. Switzer served on the Council of the ABA Section on Environment, Energy, and Resources, and the ABA Standing Committee on Environmental Law. She has authored numerous articles and books on regulatory compliance, and is a frequent writer and lecturer on GRC issues.

Anthony Tarantino, PhD, is currently with IBM's Governance, Risk, and Compliance Center of Competence. Dr. Tarantino has 30 years of experience in business transformation and compliance on both the consulting and business side. He became a six sigma black belt in 2006. His articles have been published in *Accounting Today* and *Cutter IT Journal*, as well as by the Institute of Supply Management (ISM) and Oracle Applications Users Group (OAUG). He is a regular speaker for ISM, OAUG, and Association for Operations Management (APICS) conferences and events. He is the author of *Manager's Guide to Compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, Basel II, OMBs A-123, ASX 10, OECD Principles, Turnbull Guidance, Best Practices and Case Studies* (John Wiley & Sons, 2006).

Shirley (Xuelian) **Cui Tarantino** has been a senior account executive in a compliance lab for six years. With excellent customer relationships and over $1 million in sales track records, she has liaised with international regulatory bodies and established communication channels with agencies and laboratories globally, such as the FCC, ACTA, UL, Industry Canada, CSA, European Union, China CCC, SRRC, MII, Japan TELEC, VCCI, Korea MIC, RRL, Taiwan DGT, BSMI, India WPC, TEC, Singapore iDA, Hong Kong OFTA, Philippines NTC, Malaysia Sirim, Thailand TOT, Indonesia DG PosTel, Vietnam DGPT, Mexico NOM, COFETEL, Brazil ANATEL, Argentina CNC, Chile SUBTEL, South Africa ICASA, Russia GOST, Australia/NZ ACMA, and U.S. Department of Energy (DOE), as well as the U.S. Environmental Protection Agency (EPA) for the lighting efficiency Energy Star program. She has obtained her chemical engineering BS degree in China and computer information systems MS degree from the U.S. Florida Institute of Technology.

Jeffrey C. Thomson is the Vice President of Research and Applications Development at the Institute of Management Accountants (IMA), the world's leading association for management accountants focused on driving business performance in the areas of decision support, planning and control. Jeff conceived and launched the IMA Research Center of Excellence, which has delivered practical applications, tools, and guidance, enabling management accountants to be

more successful strategic, business partners. He is also responsible for guiding the association's global strategic planning, efforts. Prior to his IMA assignment, Jeff worked at AT&T for over two decades where he served in various financial, strategic, and operational roles. He has written articles, served as a contributing author, and spoken globally on the following topics: enterprise risk management, internal controls, business performance management, strategic costing methods including activity-based costing, lean accounting, strategic planning, and competitive analysis. He has granted interviews, and is frequently quoted in The Wall Street Journal, Business Week, Compliance Week, Global Risk Regulator, and other media outlets, as well as participating in Congressional Staff Briefings on topics of interest to IMA members. Jeff has an MS in Statistics from Montclair State University, has studied Finance and Accounting at the Wharton School, and attended the Columbia University Senior Executive Leadership Program.

Brett Trusko, PhD, is a world renowned six sigma Master Black Belt who has until recently led the Process Quality Group for a major international consulting firm. His current position is as a quality researcher at the Medical College at the Mayo Clinic. He is the author of hundreds of articles on quality and as a futurist and has recently published a book, *Improving Healthcare Quality and Cost with Six Sigma*. He speaks and lectures globally on six sigma and his new approach, Dynamic Six Sigma. He has degrees in Biology, Accounting, New Product Development and a PhD in Information Technology Management.

Shann Turnbull has been chairman and/or CEO of listed companies and has founded a number of businesses, with three becoming publicly traded (refer to www.linkedin.com/pub/0/aa4/470). In 1975 he founded the first educational qualification in the world for company directors. From his PhD thesis (available at http://ssrn.com/author=26239) he created an MBA course for evaluating and designing the governance architecture of listed corporations, nonprofits, or public sector organizations. He is the author of *Democratising the Wealth of Nations*, *A New Way to Govern: Organisations and Society after Enron*, and many other writings on reforming capitalism. His professional affiliations are listed at www.aprim.net/associates/turnbull.htm

Marco Venturini was born in Milan in 1976. In 2001 he received a degree in business administration at Cattolica University, Milan. He then started his professional experience at PricewaterhouseCoopers as an auditor. In 2003 he joined an Italian diagnostic instruments group as administration manager, in charge of the administrative department and dealing mainly with costs analysis and the monthly reports for three companies controlled by the group. Since 2005 he has been working within the Italian branch of the U.S. multinational Otis Group (a United Technologies Corporation company), the world's largest manufacturer of elevators, escalators, travelators, and other horizontal transportation systems. He is the reporting manager for Ceam (an associated company of Otis Italia), responsible for the monthly financial report to the U.S. headquarters.

Hrishikesh D. Vinod worked at Bell Laboratories and was an expert witness in antitrust trials. The Maharashtra Foundation honored him for outstanding social service. Vinod started a worldwide anticorruption project in 1993. In 2005 he organized an international conference on entrepreneurship and human rights. He has published over a hundred peer-reviewed articles in econometrics, statistics, and business journals. In 1996, he was named a fellow of the *Journal of Econometrics*. Vinod has co-authored a Marcel Dekker book, *Regression Methods*, and a Wiley monograph, *Downside Risk in Stock Market Investing*. He co-edited a *Handbook of Statistics* volume with C. R. Rao.

Lawrence Wasserman, PhD, serves as President of Fortech International, Washington, D.C. Fortech is an international development firm with focus on providing technical and innovative business program support and assistance to public and private institutions. We specialize in mobile technology applications which include mobile learning, mobile marketing, and representative of products such as Learning Mobile Author software. Dr. Wasserman has worked over 20 years in Asia, Africa, and Eastern European countries. As policy management specialist, corporate governance rules and regulations assessment to measure the impact of government regulatory laws on public and private sector is a primary area of interest as well as the need for training. He has a PhD in Public Administration: Technology of Management which provided him with broad technical analysis background and governance expertise.

Liv Watson is the Vice President of Global Strategy at EDGAR Online Inc. (Nasdaq: EDGR) where she is responsible for developing EDGAR Online's International business development strategy. EDGAR Online is a leading provider of value-added business and financial information on global companies to financial, corporate, and advisory professionals. The company makes its information and a variety of analysis tools available via online subscriptions and licensing agreements to a large user base. She has spent the last 15 years finding new ways to apply her financial and business reporting expertise to technology and her technical expertise to accounting. Working globally with leading market regulators, accounting associations, and institutions, Ms. Watson has been instrumental in the creation of the XBRL International framework for the financial and business reporting supply chain. Liv has presented XBRL to a wide range of audiences from international standards bodies to Fortune 500 companies and speaks with authority about its benefits, potential applications, and broad adoption. Liv authored one of IMA's most successful CPE courses "Accounting System Technology for the 21st Century." She has also authored several published articles on future trends of the profession for international publications and journals including *Harvard Business Review* and *Strategic Finance* and writes a monthly column of financial and business reporting trends for *CPA2Biz.*

Elionor Weffort graduated in Law and holds a PhD in Accounting from the University of São Paulo/Brazil. She has worked as a lawyer and business consultant for the last 15 years. As a professor, she teaches and develops research

in International Accounting at FECAP–Alvares Penteado Business School and Fipecafi International Accounting Research Group. Elionor is the author of the book *Brazil and Accounting Harmonization: Influences of Legal and Educational Systems, Culture, and Market Forces* (PricewaterhouseCoopers Academic Series) and has published her research in several journals.

Mike Willis has more than 26 years of accounting and auditing experience and is a partner with PricewaterhouseCoopers. Mike served as the Founding Chairman of XBRL International (http://www.xbrl.org), which is currently composed of more than 500 leading software, accounting, and finance companies from 27 countries around the world. Mike has served in a number of roles within the XBRL community and currently serves on the International Steering Committee. XBRL is an international information format standard designed to dramatically enhance business reporting supply chain processes benefiting preparers, distributors, aggregators, and consumers of this information. He speaks frequently, publishes papers, and blogs on the topic of business reporting. Mike has been interviewed for or published articles in a range of business periodicals on the topic of a more efficient business reporting supply chain including the *Harvard Business Review*, *Financial Times*, *Business Week*, *Wall Street & Technology*, *CFO Magazine*, and *CIO Magazine*.

Michael P. Wilson, PhD, MPH, is an assistant research scientist at the Center for Occupational and Environmental Health, School of Public Health, University of California, Berkeley. His research focuses on the global chemical production system and on drivers of green chemistry innovation in the United States. He is the chief author of the UC Special Report, *Green Chemistry in California: A Framework for Leadership in Chemicals Policy and Innovation*, commissioned by the California Legislature in January 2004. Dr. Wilson earned a PhD in environmental health sciences from UC Berkeley in 2003, an MPH in industrial hygiene from UC Berkeley in 1998, and a BA with thesis honors in biology from the University of California, Santa Cruz, in 1984.

Markus F. Wissmann is a researcher at WHU—Otto Beisheim School of Management in Koblenz, Germany, where he conducts his work in the Group of Research in Industrial Dynamics (G/R/I/D). He studied business administration at the University in Essen (Germany) and University College Dublin (Ireland). He holds a master's degree in business and worked in an international auditing company for several years. Recently, he completed his German tax consultant diploma. He is an expert in international corporate governance issues as well as German tax laws.

Kouji Yamamoto is a director of BearingPoint Co., Ltd. He started at KPMG AZSA & Co., a Japanese member firm of KPMG International (formerly Asahi Shinwa & Co.), as a CPA. He advises corporate clients on early disclosure, implementation of consolidation systems, implementation of shared service, business process reengineering for accounting processes, preparation for internal control, implementation of impairment accounting, convergence between IFRS

and Japan GAAP, and so on. He has also written "Shareholder's Value Management," "Early Disclosure Management," "Impairment Accounting Management," and other articles that have appeared in accounting publications in Japan.

Jackie Young, PhD, after a successful career as a financial officer in the South African Defence Force, joined Standard Bank of South Africa as a management consultant. During this period he gained valuable experience on a variety of banking activities and was transferred to Group Risk Management in 2001, where he was involved in the development and implementation of a groupwide operational risk management framework. He is currently involved with the University of South Africa and consults to various businesses on operational risk management. He also wrote the book *Operational Risk Management: The Practical Application of a Qualitative Approach* (Van Schaik Publishers, 2006).

CHAPTER 1

INTRODUCTION

Anthony Tarantino, PhD

1.1 ACT LOCALLY, IMPACT GLOBALLY

In his farewell sermon to the congregation of Mount Olive Ministries in Milpitas, California, Pastor Michael Gibson urged the congregation to act locally and that every local act would have a global impact. Mike's message was directed at expanding the faith, but the process is much the same in governance, risk, and internal controls designed to improve financial, technical, and environmental

compliance. While there are global actions such as the Kyoto environmental accords, Basel II banking accords, and the International Financial Reporting Standards (IFRS) emerging as a global GAAP (generally accepted accounting principles), the vast majority of actions will occur at a local level. The cumulative effect of local actions, even though they seem insignificant, will be to improve governance, risk management, and compliance (GRC) on a global level. In short, there is no such thing as an isolated event in improving GRC. Unfortunately, this process also applies on the dark side as well. Local acts of fraud, corruption, censorship, intolerance, and other constraints on human rights do not occur in isolation. They impact us all, at least indirectly.

The process of improved GRC is and will continue to be irrevocable and irresistible. The market, political, social, and religious forces in play are all pointing in one direction. Although there is major resistance to improved GRC, ultimately the laggards will be compelled to fall in line or suffer financial, political, social, and environmental disasters and scandals that are viewed as more painful than the cure. The loss of reputation and the ostracism will also assert as great a pressure as the threats of criminal prosecution or civil litigation.

This book presents examples on national, regional, technical, environmental, and industry levels of success stories and failures in the GRC process. The goal is to provide a handbook that touches the current state, major trends, best practices, case studies, and benefits of getting there sooner rather than later.

The terms *governance*, *risk*, and *compliance* are in widespread use, and the distinctions are sometimes blurred. Internal controls and globalization are also included in many GRC-related discussions. A short explanation of each and their relationships to one another may help clear the air.

1.2 GOVERNANCE

(a) INTRODUCTION. Corporate Governance. Corporate governance addresses the processes, systems, and controls by which organizations, both public and private, operate. Governments often administer these processes and systems. The Latin origin of the word *governance* denotes steering, and governance typically includes the exercise of legal and regulatory authority and the use of institutional resources to manage organizations. It is also an area of economics that studies issues relating to the separation and segregation of ownership and control. Governance relationships include those between board directors, owners, managers, employees, suppliers, customers, regulators, and communities.

Corporate governance is the process by which an organization defends the interests of the stakeholders, which can include board members, company executives, employees, stockholders, suppliers, customers, and the community in which the organization operates. Governance refers to the relationship between those who govern and those who are governed. On a political level it is the relationship between the government and its citizens and includes three requirements:

(1) to know the present state, (2) to know where it needs to go, and (3) to know how it is progressing in the journey—somewhat analogous to what consultants call a gap analysis. It also involves three areas of decision making: who is governing, who is being governed, and what resources/assets are to be deployed in the process. The requirements and decision making apply to governments and corporations alike.

The Corporation. In 1794, Stewart Kyd created a definition of the corporation that is still valid today: "a collection of many individuals united into one body, under a special denomination, having perpetual succession under an artificial form, and vested by the policy of the law with the capacity of acting in several respects as an individual."[1] The notion of the modern corporation came into being in the aftermath of the stock market crash of 1929 and the Great Depression of the 1930s that started in the United States but quickly spread to Europe and eventually to most of the world. The scars of these two events have influenced all following generations and laid the foundations for government regulations and corporate governance. The pioneering work of Adolf Augustus Berle and Gardiner C. Means, *The Modern Corporation and Private Property* (Macmillan, 1932), continues to influence current thinking.

A corporation is an artificial legal entity, known as a juristic person under the law, which has a separate legal entity even though it is made up of a variety of other legal entities and real people. The corporation therefore has legal rights and obligations. Modern corporations typically have the following abilities and legal rights:

- Ability to access the courts (i.e., the right to initiate lawsuits and be the subject of lawsuits)
- Ability to hold assets separately from its members' assets (i.e., the right to a common treasury)
- Ability to hire and fire employees (i.e., the right to engage agents)
- Ability to enter into contracts (i.e., the right to a common seal)
- Ability to govern the corporation's internal affairs (i.e., and the right to make bylaws)
- Ability to transfer shares without impacting the existing corporation
- Ability to maintain a perpetual succession regardless of the withdrawal or removal of any of its members
- Ability to limit the liability of stakeholders[2]

The Corporation as a Legal Entity. Corporations are given a unique legal personality under the law in which shareholders own the corporation as a legal entity, but the corporation as the legal body owns the corporation's assets. Under the law, corporations have the same contractual rights as an individual and are capable, like an individual, of making contractual agreements, buying and selling real estate, and engaging in lawsuits.

While the corporation has its own existence and personality under law, it is only an abstraction and requires the actions of real people to operate. Therefore corporate law requires a board of directors to govern the organization, who delegate operational control to professional managers, typically under a chief executive officer (CEO). In some cases the CEO is also the chairman of the board of directors. The CEO-dominated corporate model evolved in the past 50 years in the United States and is sometimes referred to as the imperial CEO. In earlier times boards were dominant over corporate management, and now the pendulum is swinging again in the direction of greater board involvement and control at the expense of the CEO.

Under the law, there are three actors in corporations: directors, employees, and shareholders. Directors provide the oversight and stewardship over all corporate assets, both human and otherwise. Employees do the day-to-day work of managing the corporation's resources and assets. Shareholders provide the money in the form of risk capital and share risk equal to their investments. Shareholders' involvement in corporate operations is typically limited to interaction with the board, and not with corporate employees.[3]

The Corporation as an Economic Entity. The corporation is also an economic enterprise that exists to make profits, which are, in turn, ultimately shared with shareholders as dividends and rising stock prices. This economic entity replaces a wide variety of less efficient activities in the marketplace that would be conducted by individuals. Corporations increase efficiency by acting as independent holders of property rights that create contractual arrangements with other parties. This greatly reduces the costs and number of transactions for all those involved—customers, suppliers, employees, owners, government agencies, and so on. The separation of control and ownership, while improving efficiency, does mandate a governance framework to align corporate decisions with the corporation's economic capital and resources.

The Corporation as an Accounting Entity. Corporations are also accounting entities. Accounting is the process by which corporations identify, measure, and communicate information that impacts financial reporting. It is used by stakeholders to guide their judgment as to the current state and future prospects of corporations. Many corporate governance issues revolve around accounting-based information.

The Corporation as a Cultural and Socially Responsible Entity. Corporations are also cultural entities that often transcend national and regional borders. As global trade, politics, entertainment, media, the Internet, and other cross-border activities expand, corporations take on more of a cultural identity that is bigger than their traditional branding. Coke, Pepsi, Visa, Disney, Levi's, and IBM have been widely recognized brands in every region of the world for decades, and new names such as Apple/iPod, Yahoo!, and Google have become cultural phenomena that are growing in importance beyond traditional corporate branding.

The actions of these marquee global corporations are becoming as important as the actions of any of their home governments in shaping our lives, regardless of whether we are direct customers of their products. Consequently, the governance of these corporations takes on major significance and may trump national government regulations and regulators in shaping our economic growth and stability.

The latest example of this can be seen in the greening of corporate America. While the European Union (EU) and its resident corporations have strongly embraced improved environmental governance (discussed in detail in Part Five, our environmental compliance section), the United States has lagged in many critical areas due to the resistance of the central/federal government. (We should note that many U.S. state and local governments are taking proactive measures on their own, such as my home state of California.) Corporate America has now embraced green as good business and the socially responsible course of action—in spite of the lack of action on the federal government's part. This is counter to the notion that government should lead and that corporations are too market-driven to take such socially responsible actions. Toyota's visionary embracing of hybrid technology is one of the best examples. Toyota went to market with the Prius hybrid car even though there was no strong business reason to do so. Now all the laggards are chasing the Prius's success, and Toyota is poised to become the world's largest automaker. Toyota's leadership had little to do with stewardship or pressure from its home government in Japan.

(b) THE MORAL FOUNDATIONS TO TONE-AT-THE-TOP. Historically, investors in most companies were individuals ranging from the very rich to the working class. Over recent decades, however, institutional investors representing insurance companies, banks, investor groups, and mutual, hedge, and pension funds have become dominant players in the market. Institutional investors have been able to advocate for stronger corporate governance and oversight. While oversight has improved, it has not necessarily improved the voice of small investors. The growth of mutual funds and pension plans has given small investors at least an indirect voice.[4]

The need for institutional investors to access equity capital on a global level has increased the demand for improved governance, typically manifested through improved financial transparency, accountability, and representation of minority shareholder interests. The process has increased demand for what is commonly referred to as tone at the top—corporate boards and executives providing the stewardship, culture, and organization committed to corporate governance. Tone at the top, as the jurist said about pornography, is hard to define, but you know it when you see it. The fundamental issue around tone-at-the-top may come down to the basic ethics and morality of those in positions of corporate power. Dr. Rick Warren, in an interview by NBC's Tim Russert in the final *Meet the Press* of

2006, discussed the three requirements for good governance: freedom of religion, freedom of information, and freedom of markets. Dr. Warren is the author of the best-selling *The Purpose Driven Life* (Zondervan, 2002) and a Protestant minister. He argues that freedom of religion is key because it provides a moral foundation to governance and that without a moral foundation capitalism is pure greed. It is a profound notion and makes a lot of sense. If there is no moral and ethical foundation to the tone at the top, rules, regulations, and sanctions will ultimately fail. Morally bankrupt wrongdoers are typically too clever and powerful to be caught.

The United States is a conflicted society as to the notion of tone-at-the-top. Survey after survey shows the great majority of Americans claiming to be Christians; evangelical Christians are a major political force in American politics; and until recently no major politician would run for office as openly agnostic or atheist. The conflict comes in the major disconnect between the claims of a moral and religious foundation to governance and actions that appear to be driven by pure greed. The late Kenneth Lay (Enron) and Richard Scrushy (HealthSouth) actually made their strong Christian convictions part of their respective defense arguments during their corruption trials. (Lay lost and Scrushy won.)

During the *Meet the Press* interview, Dr. Warren referenced a conversation he had with major leaders in China. He cautioned that they would ultimately fail in that they were embracing only one of the three requirements for corporate governance—freedom of markets. The rampant and growing corruption in the booming Chinese and Indian economies lends support to Dr. Warren's arguments that all three elements are essential.

The notion of a moral or faith-based governance is not unique to the West or to modern times. The Qur'an (the Holy Book of Islam) orders the faithful to follow the principles of shariah, which require ethical business behavior and see money as a vehicle for doing good. This is a guiding principle to 1.3 billion Muslims and can be seen in Islamic banking practices. (See our two related chapters: Chapter 43, "Islamic Finance," and Chapter 46, "Corporate Governance in Major Islamic Nations.") There are also several passages in the Old Testament warning against usury, immoral, and unethical behavior. China's Confucian philosophy calls on man to serve the good of society as the highest calling.

(c) CHRONOLOGY OF CORPORATE GOVERNANCE. There is a common misconception that corporate governance is a new concept, but its roots are as old as man. The basic concepts around corporate stewardship are 400 years old. More general concepts of governance are much older and have been debated for over 2,000 years. However, the following chronology does demonstrate a major escalation in activities in the past 10 years.

Year	Location	Event
500 B.C.	China	The Confucian Analects advocate moral government led by virtue and uniformity with the rules of propriety. The Book of Mensius advocates the rights of the governed to overthrow corrupt rulers.
31 B.C.	Rome	Although lacking some of the core characteristics of modern corporations, Roman citizens invest in business enterprises as shareholders. The government sanctions corporations.
A.D. 71	Global	The New Testament of the Bible (Matt. 25:14–30) argues that money sets us apart from the animal kingdom and makes voluntary exchanges ''more fair, less wasteful, and far more extensive''. Profit and money provide opportunities to glorify God by expanding our stewardship, meeting our needs and those of others, providing charity, and promoting the mission of the church in the world.
700	Global	The Qur'an (the Holy Book of Islam) orders the faithful to follow the principles of shariah, which require ethical business behavior and see money as a vehicle for doing good.
1600	United Kingdom and Holland	The East India Company introduces a Court of Directors, separating ownership and control.
1776	United Kingdom	Adam Smith in *The Wealth of Nations* warns of weak controls over and incentives for management.
1844	United Kingdom	First Joint Stock Company Act is enacted.
1899	Japan	The Commercial Law is enacted based on German commercial law.
1930	G10 nations	The Bank for International Settlements (BIS) is created to foster international monetary and financial cooperation—the world's oldest international organization.
1931	United States	Berle and Means publish their seminal work *The Modern Corporation and Private Property*.
1933, 1934	United States	The Securities Act of 1933 is the first act to regulate the securities markets, notably registration disclosure. The 1934 Act delegates responsibility for enforcement to the Securities and Exchange Commission (SEC).
1956	India	The Companies Act is enacted as one of the most comprehensive acts in the world.
1968	European Union	The European Union adopts the first company law directive.
1974	G10 nations	The Bank for International Settlements creates the Basel Committee to improve corporate governance and stabilize markets.
1977	United States	The Foreign Corrupt Practices Act (FCPA) is enacted to prevent bribery of foreign officials.
1985	France	Publication of the Vienot Report.

(*continued*)

Year	Location	Event
1985	United States and European Union	Five nonprofit accounting and auditing organizations form the Committee of Sponsoring Organizations (COSO) to eliminate fraudulent financial reporting.
1987	United States and European Union	The Treadway Commission reports on fraudulent financial reporting, confirming the role and status of audit committees, and develops the COSO framework for internal control, published in 1992.
1988	G10 nations	The BIS's Basel Committee issues the first Basel accord, mandating minimum capital requirements.
1990	United Kingdom	Polly Peck (£1.3 billion in losses), Bank of Credit and Commerce International (BCCI), and Maxwell (£480 million) business empires collapse, calling for improved corporate governance practices to protect investors.
1992, 1993	United Kingdom	The Cadbury Committee publishes the first code on corporate governance; in 1993, companies listed on United Kingdom stock exchanges are required to disclose governance on a ''comply or explain'' basis.
1994	South Africa	Publication of the King Report.
1994	United Kingdom	Rutteman (on internal control and financial reporting), Greenbury (on executive remuneration), and Hampel (on corporate governance) reports are published.
1995	Russia	The Russian Law on Joint Stock Companies is adopted.
1996	Russia	The Russian Law on the Securities Market is adopted.
1998	Germany	KonTraG is enacted to improve corporate governance.
1998	United Kingdom	Publication of the Combined Code.
1999	G10 nations	The Bank for International Settlements' Basel Committee releases its Basel II capital accord to improve internal controls (Pillar II) and transparency (Pillar III).
1999	Global	The Organization for Economic Cooperation and Development publishes the first international benchmark, the OECD Principles of Corporate Governance.
1999	India	Clause 49 is enacted to improve corporate governance, to go into effect in 2003.
1999	Italy	Preda Code is enacted to improve governance.
1999	Mexico	Code of Best Practices is enacted representing a first for Latin America and one of the first in the world.
1999	United Kingdom	Publication of the Turnbull guidance on internal control.
2001	European Union	The Lamfalussy report on the regulation of European securities markets is published.
2001	Russia	The Russian Law on Joint Stock Companies is significantly amended.
2001	United States	Enron Corporation, then seventh largest listed company in the United States, declares bankruptcy.
2002	Canada	The Ontario Securities Commission (OSC) enacts Bill 198—Multilateral Instruments 52-109 and 52-111 (called CSOX), which mirror U.S. Sarbanes-Oxley Act (SOX)'s Sections 302 and 404.

Year	Location	Event
2002	European Union	The Winter report on company law reform in Europe is published.
2002	Germany	Publication of the German Corporate Governance Code—KonTraG
2002	Russia	Publication of the FCSM Russian Code of Corporate Conduct.
2002	United States	The Enron collapse and other corporate scandals lead to the Sarbanes-Oxley Act (SOX).
2003	France	The Yearly Budget Law (LSF) and NRE Law are enacted to improve governance and regulatory disclosure.
2003	Spain	The Aldama Commission's report is issued to improve governance.
2003	United Kingdom	The Higgs report on nonexecutive directors is published.
2004	European Union	The Parmalat scandal shakes Italy, with possible EU-wide repercussions.
2004	United States and European Union	COSO updates its 1992 internal control framework with Enterprise Risk Management (ERM), also known as COSO II or COSO 2004.
2005	Russia	The Duma's Property Committee, Economic Development and Trade Ministry, and the Federal Services Agency enact and recommend several improvements in corporate governance.
2005	European Union	Over 7,000 EU corporations embrace the International Financial Reporting Standards (IFRS) as a means to improve and standardize financial reporting.
2006	Japan	New Corporate Law (called JSOX) goes into effect to improve corporate internal controls and governance.
2007	United States	Backdating stock options scandals impact over 140 U.S. corporations with the subversion of a pay-for-performance system designed to reform corporate compensation.
2007	United States	The U.S. Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) propose changes to the most controversial sections of the Sarbanes-Oxley Act with the goal of improving U.S. competitiveness in global markets.
2011	Global banks	Global banks are required to be live under new Basel II capital accords.

(d) COMMONLY ACCEPTED PRINCIPLES OF CORPORATE GOVERNANCE. Regardless of the national jurisdiction and local conditions, there are some principles and issues of corporate governance that have been widely embraced over the years.

Rights and Fair Treatment of Shareholders. Companies need to listen to shareholder concerns and respect their rights. This includes open and two-way communication and shareholders' involvement in general board meetings.

Roles and Responsibilities of the Board of Directors. Robust corporate boards need skilled and focused members possessing a range of experience and expertise. A healthy mix of independent members with strong credentials and internal members with company expertise is essential. It is best if the chairman of the board and the CEO positions are held by different people—a sound check and balance.

Ethical and Professional Behavior. Companies need a culture of compliance and ethics, not just a code of ethics. This flows down from the board and executives through a tone at the top and is reinforced through actions, not just words.

Financial Transparency and Disclosure. Companies need strong and well-documented processes and controls to consistently provide full transparency in financial reporting. Results need to follow accepted norms and best practices and be audited by independent internal and external experts. Internal and external auditors must be qualified and strong enough to provide brutally frank assessments without the fear of retaliation. It is also necessary to defend and encourage internal whistle-blowers, who often are the best means to uncover errors and fraud in financial reporting.

Internal Controls. Internal controls are a key component to all regimens to improve corporate governance in general, to reduce risks, and specifically to provide consistent financial transparency. Debates over the scope of internal controls have raged for decades, but most agree that internal controls that impact financial reporting fall within the scope of corporate governance. Some argue that policies, procedures, training, and whistle-blower protection impact internal controls as well. The Committee of Sponsoring Organizations (COSO) framework originally issued in 1992 and updated in 2004 is often the framework of choice for internal controls management. We argue in various chapters in this handbook that the quantification and prioritization of risks are key to successful internal controls in that higher control activities are deployed for areas with the highest potential financial impact, the greatest likeliness, and the highest level of difficulty in detection.

(e) MODELS OF CORPORATE GOVERNANCE. **Anglo-American Model.** This model typically gives priority to shareholder interests, which translates into strong pressure to innovate, compete, and grow profitability. The Anglo-American model places less emphasis on the interests of managers, employees, customers, suppliers, and the community in general. Ironically, this approach does not translate into proactive shareholder involvement in corporate governance. It is a more hands-off relationship in which a powerful CEO runs the daily operations of the organization and the board provides overarching stewardship. The U.S. scandals of the 1990s have added greater oversight to board responsibilities beyond their traditional stewardship.

The Coordinated Model. This model is prevalent in Europe and Japan. It also acquiesces to shareholder interest but gives priority to the interests of managers, employees, customers, suppliers, and the community in general. The coordinated model translates to innovation and profit growth on a more incremental level. Thus there may be slower growth in profits in the coordinated model, but corporations are less likely to suffer the failures in ethics and morality that occur in the Anglo-American model with its unrelenting demands for greater and greater profits.

The Family-Owned Company Model. In many Asian and Latin American countries, family-owned companies dominate. It is not unusual for a small number of powerful families to control a majority of public companies. Powerful families also control major corporations in Spain, France, and Italy. Notions of financial transparency that dominate corporate governance frameworks under the Anglo-American model are very difficult for family-owned companies to accept. Transparency is seen as exposing core business financials and strategies, which would benefit competitors and regulators, with few tangible benefits to the organization.

(f) AGENCY THEORY VERSUS STEWARDSHIP THEORY IN GOVERNANCE. Starting in the nineteenth century, laws were enacted in Western economies that enhanced and codified the ability of corporate boards to govern their enterprises without the direct and unanimous consent of shareholders. This was in exchange for statutory benefits such as appraisal rights. In the United States, the rights of shareholders have continued to decline as wealth and control became increasingly securitized into various corporate entities and government institutions. Corporate boards thus acted as agents for their principals, or shareholders.

American expansion after World War II through the emergence of multinational corporations saw the establishment of the managerial class. Accordingly, several Harvard Business School management professors published influential monographs studying the corporations' prominence: Myles Mace (entrepreneurship), Alfred D. Chandler Jr. (business history), Jay Lorsch (organizational behavior), and Elizabeth MacIver (organizational behavior). According to Lorsch and MacIver, "many large corporations have dominant control over business affairs without sufficient accountability or monitoring by their board of directors."

Eliot Spitzer, the newly elected governor of New York, took a very aggressive approach to ferreting out corporate wrongdoing when he was New York's attorney general. He has a portrait of President Theodore Roosevelt over his desk, and like President Roosevelt he feels that government has to take a leadership role as stewards of governance. At the beginning of the twentieth century, President Roosevelt introduced the notion that government had a stewardship responsibility over business and environmental matters. He undertook actions to

attack corporate monopolies and trusts and establish a system of national parks to protect the environment.

In the 1980s, agency theory came into prominence as an accepted approach to corporate governance—an organization is seen as a series of contracts. Agency theory has its limitations in the incomplete and asymmetric information between principals and agents. This means one party to a transaction has more complete or better quality information than the other party.

Agency theory argues that shareholder interests require protection by separation of incumbency of roles of board chair and CEO. Stewardship theory argues that shareholder interests are maximized by shared incumbency of these roles. Modern governance can be seen as a hybrid of both approaches.

Advocates of agency theory argue for greater monitoring and sanctioning of management, but there is evidence that greater monitoring has its limitations and may actually backfire. Here are some examples of agency theory versus agency reality:

Greater Board Independence

- *Assumption.* Increasing the number of independent board members improves corporate governance.
- *Reality.* Some of the greatest corporate scandals occurred in corporations with a high number of independent board members: Enron (80 percent), Tyco (65 percent), WorldCom (45 percent). Various analyses indicate no statistical relationship between board independence and firm financial performance.[5]

Pay for Performance

- *Assumption.* Compensation based on performance improves employees' contributions to the common good of their companies and/or society.
- *Reality.* Several studies suggest that good behavior is not motivated by compensation. The love of work and the good of the community are not reinforced by monetary rewards (e.g., blood donations drop when compensation is offered).[6]

Executive Compensation Transparency

- *Assumption.* With improved executive compensation transparency, employees are motivated by the potential to make such lofty salaries as they move up the corporate ladder.
- *Reality.* The disparity between employee and executive salaries has increased to such an extent that employees feel like suckers and have little loyalty to their organizations—feelings of exploitation reduce good behavior. The pay disparity between the average U.S. CEO and average

employee has increased from 25 times to 75 times over the past 30 years. When stock options are included, the disparity increases to over 200 times.[7]

INCREASED SUPERVISION AND MONITORING

- *Assumption.* Increasing the supervision and monitoring of employees will improve behavior.
- *Reality.* Employees want to act as agents and not as pawns. Various studies demonstrate that increased supervision decreases effort and loyalty.[8]

(g) SCANDALS DRIVE IMPROVEMENTS IN GOVERNANCE. History has demonstrated that improvements in governance and compliance typically come as a result of scandals. When the pendulum swings too far toward self-regulation, the freedom to act outside of the rules proves to be irresistible. The resulting scandals create a cry for increased regulation. In some cases the pendulum swings back too far in the form of excess regulation. The most recent scandals of the past decade are a case in point. This is in no way an exhaustive list, but captures one of the reasons you may be reading this book:

U.S. Savings and Loan Crisis of 1986 to 1995. Over 1,000 savings and loan institutions were closed, holding over $500 billion in assets and representing about half of the total number of savings and loans. Deregulation, changing market conditions, volatile interest rates, tax changes, and reduced regulatory capital have all been cited as causes of the crisis. According to Timothy Curry and Lynn Shibut, losses totaled over $80 billion, with public sector/taxpayer costs of $75 billion and private sector costs of $7 billion.[9]

East Asian Crisis of 1997. South Korea, Malaysia, Thailand, Indonesia, and the Philippines saw their economies severely hurt by the flight of foreign capital after property assets collapsed. This was caused in part by poor governance at a national and corporate level.

U.S. Corporate Crises of 2001–2002. The collapse of Enron and WorldCom, and the ensuing scandals and collapses of other corporations such as Arthur Andersen, Global Crossing, Adelphia, HealthSouth, and Tyco, demonstrated the weakness of corporate oversight, rating agencies, audit firms, and business press. The resulting losses impacted millions of investors and several thousand employees. The perceptions of white-collar crimes changed dramatically, with demands for and the realization of jail terms that were on a par with sentences of drug dealers, rapists, and murderers. The most notable include:

- *Enron.* Ken Lay died after he and Jeff Skilling were convicted along with two dozen lower-level participants in a scandal involving accounting tricks around off-balance-sheet arrangements; called the Republican scandal due to Bush ties.

- *Tyco.* In September 2005, former CEO Dennis Kozlowski and CFO Mark Swartz were sentenced to 8.3 to 25 years in prison and must pay $134 million in restitution to Tyco and fines of over $35 million each.
- *WorldCom.* In June 2005, a federal court awarded investors over $6 billion in settlements. The largest part of the payout will come from Citigroup ($2.58 billion) and JPMorgan Chase ($2.0 billion).
- *Adelphia.* In June 2005, John and Timothy Rigas were sentenced to 15 and 20 years in prison, respectively, for their role in looting the cable giant. The scandal drove Adelphia into bankruptcy.
- *HealthSouth.* In March 2005, former CEO Richard Scrushy, the first CEO charged under SOX, was acquitted of all charges related to a $2.7 billion earnings overstatement. He was later convicted of other fraudulent activities.

EU Scandals of 2001–2003. The Italian dairy giant Parmalat filed for bankruptcy in December 2003 after collapsing under about $18.1 billion of debt and is suing Citigroup, Bank of America, and former auditors Grant Thornton and Deloitte & Touche. Ahold, the world's third largest food distributor, lost two-thirds of its stock value in the EU's largest scandal. The scandal stemmed from accounting irregularities from a U.S. subsidiary, which overstated its income by $880 million in 2001 and 2002.

U.S. Post-Enron Scandals of 2003–2006. In March 2005, Time Warner, the world's largest media company, agreed to pay $300 million to settle federal fraud charges for overstating its Internet subscribers and revenues, leading to an August 2006 restatement of $584 million in advertising revenues. Fannie Mae paid $400 million in fines to the SEC; its losses total $10.6 billion, shareholder losses total $30 billion, 44 of 55 executives were out, and 29 may be forced to return bonuses (called the Democratic Party scandal due to close ties). Former Refco CEO Phillip Bennett was accused of hiding $430 million in debt in a post-SOX scandal. Grant Thornton is being sued over its auditing of the Refco initial public offering (IPO), which occurred in August 2005.

Financial Services Scandals of 2003–2006. The past few years have seen a wide variety of scandals:

- *Securities and Exchange Commission/National Association of Securities Dealers (SEC/NASD) and New York Stock Exchange (NYSE).* Fines of $8.5 million were levied against five brokerage firms for failure to preserve e-mail communications.
- *Credit Suisse First Boston.* Criminal charges were brought against CSFB investment banker Frank Quattrone for allegedly telling people to "clean up" files after learning about an investigation.
- *Riggs Bank.* The Albritton family lost control of Riggs Bank after various scandals and fines of $25 million.

- *BCCI.* The Bank of Credit and Commerce International (BCCI) scandal resulted in the Bank of England being sued by creditors for £1 billion ($1.8 billion).
- *Morgan Stanley.* Morgan Stanley paid a $50 million fine to settle allegations that it inappropriately steered customers into select mutual funds in exchange for secret commissions as regulators targeted the industry's controversial fee regime.
- *Morgan Stanley.* Morgan Stanley was ordered to pay billionaire financier Ron Perelman more than $1.4 billion in damages over the 1998 sale of his Coleman camping-gear company to Sunbeam.
- *Prudential Financial.* Prudential and a subsidiary agreed to pay $600 million in penalties to resolve government allegations of deceptive market timing in the trading of mutual funds.
- *China Construction Bank.* Chairman Zhang Enzhao pleaded guilty to bribery and faces life in prison.
- *Banca Popolare Italiana.* Consolidation of the banking sector in Italy has been spurred since a scandal involving BPI and others led to the resignation of Antonio Fazio.

U.S. Stock Option Backdating Scandal of 2005–2006. Over 100 U.S. companies have been implicated in cheating on the dates that stock options were granted. It took some astute mathematicians to demonstrate that it was statistically impossible that options were always granted at the lowest levels for a given period. Several executives have been indicted, and several more have been forced to resign and repay their option gains. The *Wall Street Journal* estimates 2,000 U.S. companies may be drawn in. Silicon Valley is such a target of the investigations that the Federal Bureau of Investigation (FBI) has set up a temporary office in the area. Law firms are gearing up to handle the cases and looking to make a fortune in the process.

1.3 RISK

(a) INTRODUCTION. Definitions of risk typically refer to the possibility of a loss or an injury created by an activity or by a person. Risk management seeks to identify, assess, and measure risk and then develop countermeasures to handle it. This typically does not mean eliminating risk but rather seeking to mitigate and minimize its impact. Risk should not be viewed as inherently bad. All opportunities come with some degree of risk. An organization that is totally risk averse is not likely to be very attractive to investors and may be doomed ultimately to fail.

Just as risk and opportunity go hand in hand, risk, compliance, and internal controls go hand in hand. The process an organization, its internal auditors, its external auditors, and its regulators would typically follow to validate

the effectiveness of internal controls in controlling risk would include these elements:

- Identify business processes, especially those impacting financial reporting.
- Identify the risks associated with each process.
- Identify the internal controls used to mitigate the risks for each process.
- Create a hierarchy of business processes, risks, and controls.
- Identify the tests to be used in determining the effectiveness of the internal controls.
- Test the internal controls and publish findings.
- Provide an opinion as to the effectiveness of the controls.
- If the controls are found to be ineffective, recommend changes (remediations) and retest the controls.
- Create and maintain a documentation library of the processes, risks, controls, tests, findings, remediations, and so on involved in the risk/control process. This would include a risk/control matrix, process narratives, process flow charts, test procedures, and so forth.
- If the internal controls are found to be effective, business owners and external auditors sign off as part of a certification process.

The types of risks that impact companies vary depending on the home country location, industry, level of globalization, and many other factors. Banks worry about credit and market risks. Many firms worry about reputation and legal risks. Risks can be internally or externally based, but one area of risk impacts all companies: operational risk.

Banking is addressing operational risk in a big way with its new capital adequacy accords known as Basel II. Basel II defines operational risk as the risk of losses resulting from inadequate or failed internal processes, people, and systems or from external events. Although designed for banking, this definition holds true for any industry. Basel II describes seven major areas of operational risk:

1. Internal fraud
   - Unauthorized activities
   - Theft and fraud
2. External fraud
   - External security
   - Theft and fraud
3. Employment practices
   - Employee relations
   - Safe environment
   - Diversity and discrimination
4. Clients, products, and business processes
   - Suitability, disclosure, and fiduciary aspects

- Product flaws
- Improper business or market practices
- Advisory activities
- Selection, sponsorship, and exposure

5. Damage to physical assets
   - Disasters and other events
6. Business disruptions and system failures
   - Systems
7. Execution, delivery, and process management
   - Transaction capture, execution, and maintenance
   - Monitoring and reporting
   - Incomplete legal documentation
   - Customer account management

(b) COSO AND ENTERPRISE RISK MANAGEMENT. In 2004, the Committee of Sponsoring Organizations (COSO) published an update to its 1992 risk management framework. Known as Enterprise Risk Management (ERM), it added the concept of event management and recognized that controls will differ from the top of an organization down to its operational/local levels—a strategic versus tactical approach.

There are eight interrelated components that make up ERM. The eight components are based on an organization's management approach and processes. The components are:

1. *Internal environment.* New to ERM and not part of COSO 1992, this covers the tone at the top of an organization, and includes the philosophy around risk appetite, ethics, and in turn the environment in which they operate.
2. *Objective setting.* New to ERM and not part of COSO 1992, this covers the identification and prioritization of objectives. The goal is to have in place objectives that are in alignment with the organization to ensure that management has a set of risk management objectives that are in alignment with the company's overall mission and goals.
3. *Event identification.* New to ERM and not part of COSO 1992, this covers the management of internal and external events affecting achievement of an organization's objectives. The traditional thinking treated risks and controls as a static situation. The original framework did not distinguish between controls to manage recurring processes and controls for one-off events like natural and man-made disasters.
4. *Risk assessment.* Part of COSO 1992, this covers the analysis and rationalization of risks as to their likelihood and their financial impact, and the

nature of the controls needed as a basis for determining how risks should be managed. Risks are assessed on an inherent and a residual basis. Inherent risk management (sometimes called gross or absolute risks) assesses the consequence and likelihood of a risk occurring before any controls are taken into account. Residual risk management (sometimes called net or controlled risks) assesses the consequence and likelihood of a risk occurring after any controls are taken into account.

5. *Risk response.* Part of COSO 1992, this covers management's response to risk—avoiding, accepting, reducing, or sharing risk—developing a set of actions to align risks with the entity's risk tolerances and risk appetite. An important part of risk response is evaluating the cost versus benefits of the various risk management alternatives. It is impossible to eliminate all risks, and some countermeasures may be prohibitively expensive, especially for manual controls. Automating manual controls is usually a good option that lowers risks as well as auditing and related compliance costs.
6. *Control activities.* Part of COSO 1992, this covers policies and procedures established and implemented to help ensure the risk responses are effectively carried out. Auditors would typically test to determine if policies and procedures are being followed and whether they are effective in controlling risks.
7. *Information and communication.* Part of COSO 1992, but greatly expanded in ERM, this covers how relevant information is identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
8. *Monitoring.* Part of COSO 1992, but greatly expanded in ERM, this covers the entirety of enterprise risk management—how it is monitored and how modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.[10]

(c) INFORMATION TECHNOLOGY (IT) RISK MANAGEMENT. Risk management for information technology (IT) is a growing challenge as GRC requirements expand at an exponential rate and impact all areas of IT. The high turnover rates for chief information officers (CIOs) and chief technology officers (CTOs) are evidence of the increasing burden and stress placed on IT organizations. As pressure mounts on financial officers, they make ever greater demands on IT to improve the timeliness, accuracy, and cost of storage, archiving, encryption, searching, retrieval, consolidated financial reporting, dashboards, alerts, document and records management, e-mail and instant messaging controls, and so on.

The National Institute of Standards and Technology (NIST) has statutory responsibilities in the United States under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996 to provide

IT guidelines for U.S. federal agencies. NIST's Special Publication 800-30 (*Risk Management Guide for Information Technology Systems*, July 2002) provides IT risk management recommendations that are a good foundation for any IT organization to follow. NIST's 800-30 stresses the important role risk management plays in protecting an organization's information assets. It warns that IT risk management should not be treated as primarily a technical process of IT, but as an essential control function that all business owners must support across any organization. Three basic processes are involved:

1. *Risk assessment.* This includes identifying and evaluating risks and risk impacts, and recommending measures to reduce risks.
2. *Risk mitigation.* This includes the prioritizing, implementation, and maintenance of the appropriate measures to reduce risks recommended in the risk assessment process.
3. *Evaluation and assessment.* This includes the continual evaluation process and the keys for implementing a successful IT risk management program.[11]

This is very much a balancing act in that absolute control measures are often cost prohibitive and require IT professionals to weigh the cost versus benefits of a myriad of options available to them. This process is complicated by the hundreds of software tool suppliers in the market promising to fix their GRC problems, conflicting demands from various parts of the organization, and a ratcheting up of requirements driven by litigation as much as by regulations.

Legal Discovery Demands on IT Risk Management. Legal discovery presents an especially difficult challenge. Most major lawsuits involve major requirements to produce electronically stored information (ESI). The United States, as potentially the most litigious society in history, is leading the charge. On December 1, 2006, the U.S. Supreme Court approved new Federal Rules of Civil Procedure to provide a standard for the legal discovery around ESI. The rules are important as they are bound to followed elsewhere and because American-based litigation will impact many non-American corporations doing business with the United States. They can be summarized:

- *Early attention.* Rule 26(a)(1) requires each party to show what information they have in their possession. Rule 26(f) requires the parties to come to a consensus as to what information will be in scope.
- *Form of production.* Rule 34(a) and (b) permit each party to request all types of electronically stored information—no ESI can be automatically excluded. Rule 26(b)(5)(B) requires parties to return or destroy privileged information that is uncovered in the discovery process.
- *Sanctions.* Rule 37 protects parties from being sanctioned for purging data as part of their normal operations.

- *Accessibility.* Rule 26(b)(2)(B) provides protection from prohibitively costly discovery requests. In the past, parties could make unrealistic demands to produce huge volumes of documents and records.

There are several other document and records management standards and guidelines that increase demands on IT risk management of ESI:

- Department of Defense (DOD) Directive 5015.2
- The United Kingdom's The National Archives (TNA)
- Germany's Document Management and Electronic Archiving (DOMEA)
- Australia's Victorian Electronic Records Standards (VERS)
- Canada's Electronic Records as Documentary Evidence
- ISO 15489, Information and Documentation on Records Management Guidelines
- The European Union's Model Requirement for the Management of Electronic Records (MoReq)
- The SEC's Section 19(b)(3)(A) and 19b-4(f)(6) to show all stock bids and offers

The cumulative effect of these higher standards and the growing complexity of litigation will be to substantially increase demands on IT risk management. Ironically, the give-and-take of lawsuits will drive the process ahead of regulations. In the United States, there are no hard-and-fast rules as to what is an acceptable response time to produce electronically stored information. As one party demonstrates the ability to produce ESI in a few days or weeks, the other parties will be under growing pressure to move as quickly or face losing their case before it begins.

Key Roles in IT Risk Management. The key stakeholder roles in supporting information technology risk management can be summarized:

- *Senior management.* Senior management should ensure that the needed resources are applied to develop the capabilities to accomplish the company's strategic objectives. This includes evaluating risk assessments and incorporating the results into the company procedures and the decision-making process.
- *Chief information officer (CIO).* The CIO is responsible for the company's IT budgeting, planning, and performance, including the elements of its information security systems and assuring that decisions have an effective risk management foundation.
- *Information and system owners.* Information and system owners need to ensure that the appropriate controls are deployed to assure the availability, integrity, and confidentiality of the IT data and systems they are responsible for. It is essential that they understand and accept their role in the IT risk management process.

- *Functional and business managers.* The functional and business managers who purchase and use IT also have a critical role in the IT risk management process. They need to determine a variety of trade-offs between their users' demands and security requirements.

(d) QUANTIFICATION OF RISK. A major theme of this handbook is the criticality of quantifying risk. The original and revised COSO frameworks, while important contributors in improving corporate governance, lack a viable framework to quantify risk. Part of the problem stems from the overreaction that the U.S. Sarbanes-Oxley Act brought to the risk management process. Regulators and auditors, fearful of losing investor confidence, imposed draconian measures requiring the internal testing of controls and an independent retesting of the same controls by external auditors. Even though Section 404 did not mandate this level of micromanagement, in practice auditors tested all controls, regardless of the level of risk. If the audit community had considered a six sigma and statistical approach, they would have been able to apply simple quantitative models to measure and rationalize risk. The process could be as simple as applying three variable factors to all risks:

1. Financial impact
2. Likeliness of occurrence
3. Inability to detect

A simple 1 to 10 scoring would be applied to rate each risk. For example:

1. Financial impact = 10
2. Likeliness of occurrence = 6
3. Inability to detect = 6

In this example, the risk has a score of 22 out of a maximum possible of 30 and a minimum score of 3. Such a risk should be given much more attention than risks with very low scores. History has taught us that the Italian economist Vilfredo Pareto was right in developing his 80/20 rule. The good news is that in most cases, 20 percent of the total population of risks will represent 80 percent of the potential risks. Accountants knew this well when they developed the general rule of thumb known as the 5 percent rule. They would not focus on risks that impacted less than 5 percent of financial results. By doing so, they eliminated low-value activities and could focus on the significant few items representing the great majority of income and expenses.

1.4 COMPLIANCE AND INTERNAL CONTROLS

(a) INTRODUCTION. *Compliance* is a fairly straightforward concept of acting in accordance with established laws, regulations, protocols, standards, and specifications. The critical issue is around the cost of noncompliance, which can be civil,

criminal, reputational, financial, or market based. Corporate compliance typically includes compliance with external laws (enacted by legislative bodies) and regulations (created by regulatory bodies) and internal protocols such as policies and procedures.

Internal controls is a term in widespread use around financial reporting, but it can also be applied to technical and environmental compliance. The adoption of risk management frameworks like COSO (developed by the Committee of Sponsoring Organizations) in 1992 has given the concept of internal controls a great deal of attention. Several financial control regulations have embraced a COSO or COSO-like approach to internal controls. Internal controls typically include a process, affected by an organization's board of directors, management, business owners, and technology users, which is designed to provide reasonable assurance in achieving the following objectives:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Laws and Regulations. Compliance and internal controls are needed to meet a growing number of laws and regulations. As mentioned, laws are enacted by legislative bodies, while regulations are created by government agencies. For instance, the U.S. Congress passed the Sarbanes-Oxley Act in 2002. The act is quite short with few specific or actionable details. The law called on the Securities and Exchange Commission (SEC) to create a body of regulations to apply the law to public and private U.S. companies and to foreign filers in the United States. Section 404 is an example of a regulation created by the SEC to apply the Sarbanes-Oxley Act—a law. Typically regulations are much more detailed than their parent laws.

Standards. Compliance and internal controls are also to meet a growing number of internationally accepted standards. While standards do not have the force of law, many laws and regulations will reference acceptable standards. For example, the COSO risk management framework is referenced by the SEC as an acceptable framework for risk management. This is not at the exclusion of all other frameworks. The SEC also references the UK's Combined Code as an acceptable risk management framework.

(b) THE CASE OF SARBANES-OXLEY SECTION 404. The most controversial law, regulation, and standard of the past decade have been, respectively, the enactment of the Sarbanes-Oxley Act (SOX) by the U.S. Congress in 2002; the SEC's creation of a regulation over internal controls attestations as part of Sarbanes-Oxley, Section 404, in 2003; and the creation of Audit Standard Number 2 for Internal Controls, under Section 404, by the Public Company Accounting Oversight Board (PCAOB) in 2004. While the great majority of Sarbanes-Oxley has been very well received, this one section has created quite a flap. Ironically,

the law and even the regulation are not at issue. It is how the PCAOB decided to create Audit Standard Number 2 and how audit firms in turn decided to meet the audit standard. After the demise of Arthur Andersen and widespread fear of litigations by angry shareholders, audit firms were naturally very concerned over their survival and tended to err on the side of caution by testing controls even for processes that were of low value and not critical. This was also a self-serving approach, as it resulted in a doubling of audit fees compared to the pre-Sarbanes-Oxley era.

The relationship of the U.S. law to the SEC regulation and to the PCAOB audit standard demonstrates how well-intentioned measures to improve GRC by legislators and regulators can backfire. The SEC continues to struggle with defining guidelines that strike a balance between good governance and the cost of compliance. The controversial audit standard of Section 404 is being fundamentally rewritten as Audit Standard Number 5 and a companion audit standard to rely on the work of others. This is due to widespread criticism. Other evidence of the unforeseen consequences can be seen in the two-year delayed implementation of Section 404 for smaller companies and foreign filers.

Critics claim that Section 404 has damaged entrepreneurship by denying access to capital markets and driving initial public offerings (IPOs) offshore. As we discuss in our U.S. corporate governance chapter (Chapter 66) and in the section on globalization of capital markets in this introductory chapter, the truth is not this simple. Defenders of the regulations claim that the United States continues to attract global capital because of higher corporate governance standards. Private equity firms have enjoyed major increases in activities, but it is difficult to argue that this is direct result of higher U.S. compliance costs. In the year from October 31, 2005, to October 31, 2006, over 2,000 buyouts occurred globally with a value over $500 billion—up from $291 billion in the prior year.[12]

One of the worst unforeseen consequences of the law, the regulation, and the audit standard has been on small and midsize enterprises (SMEs), typically under $700 million in public float. The cost of compliance was never calibrated for the little guys. Legislators, SEC officials, and PCAOB audit authorities never seemed to grasp that small companies could not afford the large overhead and bureaucracy required to comply with the law, the regulation, and the audit standard.

Maybe the most valuable lesson of the U.S. experience is that GRC overreactions are bound to create unforeseen and unwanted consequences. While most reforms are scandal or crisis driven, it is essential that political, legal, and business leaders calm public fears and ponder their actions carefully. The intent of the U.S. Congress and President George W. Bush was to restore investor confidence after a series of highly publicized corporate scandals hurt thousands of employees and millions of investors. It was not their intent to add a heavy regulatory burden on companies, especially smaller companies. Greater emphasis on improved board governance, transparency, and accountability would produce better results than

improved internal controls. This can be seen in the high World Bank governance scores achieved by Canada, Australia, Germany, and the UK (described in the next section) with their strong board governance codes and without an equivalent to Audit Standard Number 2.

The disconnect between the intent and the reality of Sarbanes-Oxley can be seen in the SEC's original estimate of its costs. In its final ruling on Section 404, the SEC estimated the act would require about one full-time equivalent (FTE) internal resource and about one-half FTE external resource. With minimum costs running over $5 million for most larger companies, the SEC estimate looks very naive in hindsight. It was apparent after the first year of audit activities that the SEC had terribly underestimated the internal and external costs of complying with the act, yet there was little action by the SEC or PCAOB to address the excessive costs.

The U.S. experience teaches us that there must be an active two-way communication of *all* stakeholders from the legislative process down through the regulatory process and finally to the standards process. The circle of stakeholders is larger than one might imagine and should include business owners of the processes audited. Business owners understand better than any auditor the risks associated with the business processes within their span of control. They should be the first stop in determining the level and nature of controls and audit test procedures. These business owners need to represent the entire spectrum of business activities, from the very large global firms to the small entrepreneurial firms that are the engine of growth in much of the world.

Because boards and executive management were slow to grasp the huge impact on their organizations, they did not instill in their business process owners a sense of ownership with regard to compliance. In the early days, it was looked at as yet another regulatory pain in the neck. With the proper tone-at-the-top, management training, and reorganization, American companies could have been much more proactive in pushing back on what is now seen as many silly compliance requirements with little impact on financial reporting.

Banking's Basel II accords are not a bad role model to follow in the laws to regulations to standards process. The banking industry has had about eight years to prepare for the new minimum capital requirements developed by the Bank for International Settlements' Basel Committee. The accords do not have the force of law and are being adopted by national legislative action. Unlike Sarbanes-Oxley, the accords are not designed for midsize or smaller banks and do not take a one-size-fits-all approach. They have been well thought out and actively discussed for years. Unlike Sarbanes-Oxley with its punitive sanctions, the accords provide financial incentives for improved compliance—lower capital costs. The major rating agencies have published position and white papers describing Basel II best practice frameworks. This is not to say that all banks are prepared for or happy with the demands of the accords, but at least they should know what is coming at them.

1.5 GRC AND GLOBALIZATION

(a) INTRODUCTION. *Globalization* can be viewed as activities that increase cross-border activities such as trade, communication, treaties, travel, and compliance protocols. For our purposes, we will measure globalization as total trade (imports plus exports) as a percent of gross domestic product (GDP). By this measure, globalization is increasing in all regions and for several decades. Governance at a cross-border and national level can be looked at as an overarching umbrella that applies to a variety of frameworks and regulations that are utilized by companies and other organizations, and then implemented at a granular level via internal controls and other compliance activities.

One of the most popular arguments for improving governance, risk management, compliance, and internal controls is that doing so will open up new markets and increase growth. A related argument is that improved governance is needed to play in a global marketplace. Our evaluation indicates that some of the fastest growing economies are laggards in improved governance, but that most of the global economies are leaders in governance and compliance.

This handbook provides essays for the top 75 percent of global GDP for purchasing power parity (PPP), comprising 16 nations from the United States to Australia. We looked at their growth in GDP, their governance ratings by the World Bank, and their level of globalization as measured by total trade as a percent of their GDP. (See Exhibit 1.1).

GDP is typically measured at either market exchange rates or PPP. We believe PPP is a better means to measure average volumes of inputs and outputs and to measure living standards. PPP is better at capturing the true value of nontradable goods and services. John Hawksworth uses the example of a haircut to make the point, noting that a haircut costing $20 in New York can be had for less than $1 in China. PPP adjusts for these differences to capture the true purchasing power.[13] So a person with $1 in China has parity with a person with $20 in New York.

Using trade as a percentage of GDP, Germany, Canada, Spain, France, and the UK are the most globalized economies among the top GDP nations, while India, Brazil, China, Indonesia, and the United States are the least.

It may seem ironic that the United States would be grouped with the least globalized economies, but it is reaching a milestone in 2007 when imports are expected to exceed federal spending for the first time in history. The slowness of the United States to adopt the International Financial Reporting Standards (IFRS) and the Basel II accords in banking, as well as U.S. rejection of the Kyoto environmental accords, are reminders that the United States is not as globalized as one might think.

(b) GLOBALIZATION OF CAPITAL MARKETS. Capitalism is on the march everywhere around the globe, even in societies such as China and Vietnam that still embrace Communism with its central planning. The combination of expanding

capitalism and global trade require global capital markets to fund infrastructure and other improvements. Global financial markets, in turn, require harmonized regulations. The largest U.S. equity exchanges are now publicly traded entities. This is also the case for most of the world's equity exchanges. Major exchanges are also in the process of mergers and acquisitions. Both of these developments would have been unthinkable a generation ago. Exchanges are now subject to the same regulations as their member firms, and the cross-border merger and acquisition activities are accelerating the push for a convergence and harmonization of regulations.

Former SEC chairman Harvey L. Pitt argues that the globalization of capital markets is making it less important where stocks are listed and more important where shares are traded.

Globalized capital markets will require some degree of regulatory harmonization. Pitt describes the three regulatory areas that require harmonization:[14]

1. *Equivalence.* Equivalence encourages regulators to create regulations and standards to address common concerns. The international adoption of the International Financial Reporting Standard (IFRS) is one of the best examples of this process. The U.S. rules-based generally accepted accounting

GDP Rank	Country	GDP (Purchasing Power Parity)	Cum. GDP %	Total Imports & Exports	Trade as % of GDP	GDP Growth Rate %
	World	**$60,630**	**100%**	**$20,630**	**34%**	**4.7%**
1	United States	$12,310	20%	$2,655	22%	1.9%
2	China	$ 8,883	35%	$1,384	16%	10.2%
3	Japan	$ 4,025	42%	$1,002	25%	2.6%
4	India	$ 3,666	48%	$ 189	5%	8.4%
5	Germany	$ 2,480	52%	$1,817	73%	0.9%
6	United Kingdom	$ 1,818	55%	$ 856	47%	1.9%
7	France	$ 1,794	58%	$ 917	51%	1.2%
8	Italy	$ 1,667	60%	$ 741	44%	0.1%
9	Russia	$ 1,584	63%	$ 370	23%	6.4%
10	Brazil	$ 1,536	66%	$ 193	13%	2.3%
11	Canada	$ 1,111	67%	$ 683	61%	2.9%
12	South Korea	$ 1,101	69%	$ 437	40%	4.0%
13	Mexico	$ 1,064	71%	$ 466	44%	3.5%
14	Spain	$ 1,033	73%	$ 544	53%	4.0%
15	Indonesia	$ 870	74%	$ 146	17%	5.6%
16	Australia	$ 636	75%	$ 223	35%	2.7%

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (September 2006).

EXHIBIT 1.1 GDP VERSUS TRADE VERSUS GDP GROWTH

principles (GAAP) are at odds with the principles-based approach of the IFRS. The U.S. system will eventually have to give way in order for the United States to remain a competitive player.

2. *Reciprocity.* Reciprocity encourages regulators to create mirror-image regulations and standards based on markets of interest.
3. *Transparency.* Transparency requires more complete financial disclosure and accountability. As we will cover in our 16 national and four regional corporate governance essays/chapters, the drive for transparency and accountability is virtually universal. No major economy is defending opaqueness and poor accountability.

The major rating agencies and audit firms are also playing a role in the globalization of capital markets by imposing best practice frameworks regardless of regulatory requirements. Banking is at the forefront of this phenomenon. While the Basel II accords only technically apply to very large global banks (over $250 billion in consolidated assets or over $10 billion in foreign exposure), rating agencies will punish smaller firms for not voluntarily complying. Many non-U.S. corporations have already felt the sting of Section 404 of the Sarbanes-Oxley Act as well. Rating agencies and auditors have come to expect SOX-like controls in areas of access and change control, segregation of duties, and documents and records management. There is now a bias in their thinking and actions in favor of higher standards, even though local regulations do not mandate them. Auditor fears of company-ending lawsuits and prosecutions are very real and not paranoia. Besides the one-count conviction that destroyed Arthur Andersen, the world's largest and most prestigious audit firm, major governance-related scandals typically include litigation against the auditors involved. Rating agencies were humiliated by their failure to see the pending disaster at Enron and other highly rated firms that crashed and burned, so their raising the governance bar is a natural defensive action.

Insurance companies are playing a role as well, insisting on proof of good corporate governance in order to secure the most favorable rates for corporate directors and officers (D&O), errors and omissions (E&O), and other types of professional liability policies. Several major pension funds from a variety of countries created a charter requiring global standards for environmental, social, and governance frameworks. These 32 funds are worth over $2 trillion, which is more money than is managed by all the world's hedge and equity funds.[15]

The debate continues in the United States as to whether overly costly regulations have hurt U.S. competitive markets and driven capital to other markets. This has been a popular argument in the United States for the past few years, but the globalization of financial markets may be the major factor, not the costs of U.S. regulations. As corporate governance improves in other markets, it is natural that companies will look to go public in their home markets. Cross-border trading

has become easier, reducing the prestige of listing on the large U.S. exchanges; and private-equity buyouts are growing in popularity on a global basis, not just in the United States.[16] Our 16 national and four regional corporate governance chapters demonstrate a virtually universal commitment to improved governance, so the benefits of a U.S. listing are bound to diminish.

(c) GOVERNANCE, TRADE, AND GROWTH. The World Bank describes six categories of governance and has evaluated over 200 countries against these standards. Its approach makes a lot of sense.

1. *Voice and accountability* measures the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and a free media.
2. *Political stability and absence of violence* measures the perceptions of the likelihood that the government will not be destabilized or overthrown by unconstitutional or violent means, including domestic violence and terrorism.
3. *Government effectiveness* measures the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies.
4. *Regulatory quality* measures the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development.
5. *Rule of law* measures the extent to which agents have confidence in and abide by the rules of society, in particular the quality of contract enforcement, the police, and the courts, as well as the likelihood of crime and violence.
6. *Control of corruption* measures the extent to which public power is prevented from being exercised for private gain, including petty and grand forms of corruption, as well as so-called capture of the state by elites and private interests.

We created a score based on an average of the six elements of governance and then placed each of the 16 nations in one of four quadrilles, with 1 the best and 4 the worst. (See Exhibit 1.2.)

The arguments about the benefits of improved governance are rather academic. To illustrate the point, take a look at some of the countries with the worst governance ratings. Only those holding power in these areas would advocate joining this list. The prestige and panache of joining the first quadrille of nations is very compelling. The social, political, and economic benefits are surely obvious.

As mentioned, we did find a direct correlation between governance and globalization by measuring quadrilles for both. In general, the leaders in good governance were also those with the highest trade activities. This makes sense,

World Bank Six Elements of Govemance	US	China	Japan	India	Gemany	UK	France	Italy	Russia	Brazil	Canada	Mexico	Spain	S. Korea	Indonesia	Australia
Quadrille	1	3	1	3	1	1	1	2	3	2	1	2	1	1	3	1
Score	84.3%	35.6%	83.3%	45.6%	88.1%	88.1%	83.6%	68.3%	29.5%	49.8%	92.3%	48.9%	83.3%	70.2%	27.5%	91.5%
Voice and Accountability	88.9%	6.3%	74.9%	55.6%	93.7%	92.8%	92.3%	77.3%	25.6%	57.0%	95.2%	54.1%	87.0%	68.1%	40.6%	94.7%
Political Stability /No Violence	48.6%	39.2%	80.2%	22.2%	67.0%	59.4%	58.5%	52.8%	18.9%	40.6%	78.8%	36.3%	60.4%	60.8%	9.0%	73.6%
Government Effectiveness	91.9%	52.2%	84.7%	51.7%	90.4%	94.3%	90.0%	71.8%	38.8%	55.0%	95.7%	57.4%	89.5%	78.9%	37.3%	94.7%
Regulatory Quality	93.1%	44.6%	85.6%	41.1%	90.1%	94.1%	80.2%	76.2%	43.6%	55.0%	95.0%	62.4%	87.6%	71.8%	36.6%	96.0%
Rule of Law	91.8%	40.6%	89.4%	56.0%	93.7%	93.2%	89.9%	64.3%	21.7%	43.0%	95.2%	39.6%	85.0%	72.5%	20.3%	94.7%
Control of Corruption	91.6%	30.5%	85.2%	46.8%	93.6%	94.5%	90.6%	67.5%	28.1%	48.3%	94.1%	43.8%	90.1%	69.0%	21.2%	95.1%

World Bank Six Elements of Govemance	Iraq — 2005	Iraq — 2002	North Korea	Iran	Somalia
Rank: 203 Ct.	202	N/A	194	172	203
Quadrile	4	4	4	4	4
Score	3.7%	1.5%	9.3%	21.6%	2.0%
Voice and Accountability	9.2%	0.5%	0.5%	9.7%	1.9%
Political Stability /No Violence	0.0%	5.2%	41.0%	16.0%	5.0%
Government Effectiveness	1.4%	0.5%	0.5%	26.3%	0.0%
Regulatory Quality	5.9%	0.0%	0.5%	6.9%	0.0%
Rule of Law	0.5%	1.9%	10.1%	29.0%	0.0%
Control of Corruption	4.9%	1.0%	3.4%	41.4%	5.0%

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (September 2006).

EXHIBIT 1.2 WORLD BANK SIX ELEMENTS OF GOVERNANCE: MAJOR GDP ECONOMIES AND LOWEST RANKING ECONOMIES

as globalized economies are very interdependent on one another. Some of the fastest growing economies lag in improving compliance. (See Exhibit 1.3.)

We did not find a direct correlation between growth and governance. China, India, and Russia are among the fastest growing major economies in the world, but lag in improving governance. (See Exhibit 1.4.)

Country Quadrille Rank	World Bank Governance (Six Elements)	Globalization (Trade as % of GDP)	Average	Standard Deviation*
United States	1	1	1.00	0.00
China	3	4	3.50	0.71
Japan	1	2	1.50	0.71
India	3	4	3.50	0.71
Germany	1	2	1.50	0.71
United Kingdom	1	1	1.00	0.00
France	1	2	1.50	0.71
Italy	2	2	2.00	0.00
Russia	4	4	4.00	0.00
Brazil	3	4	3.50	0.71
Canada	1	1	1.00	0.00
Mexico	3	3	3.00	0.00
Spain	1	2	1.50	0.71
South Korea	1	2	1.50	0.71
Indonesia	4	4	4.00	0.00
Australia	1	1	1.00	0.00
Average	**1.94**	**2.44**	2.19	0.35
Standard deviation	**1.18**	**1.21**		

*Standard deviation under 1 suggests a strong correlation.
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (September 2006).

EXHIBIT 1.3 WORLD BANK GOVERNANCE VERSUS GLOBALIZATION

1.6 GROWTH OF GLOBAL TRADE

At this point, you may be asking yourself: What does this have to do with me? The answer comes in the World Trade Organization's 2005 statistics expressed in a chart of the growth in global trade versus production. Exhibit 1.5 shows that global trade has consistently grown at about twice the rate of production for more than 50 years. In short, very few of us will operate in isolation; we will need to navigate our way through a maze of laws, regulations, and standards no matter where we live and no matter what type of enterprise or organization we are involved with.

The growth in global trade is not restricted to a few regions. Ironically, North America has one of the lowest growth rates in both imports and exports from 2000 to 2004, as shown in Exhibit 1.6.

1.7 SIMPLE SUGGESTIONS TO IMPROVE GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE (GRC)

(a) TAKE A HOLISTIC APPROACH TO GRC. Organizations. An expensive and painful approach to the subject of governance, risk management, and compliance (GRC) is to treat it in a piecemeal and disjointed fashion, as a series of unrelated

Country Quadrille Rank	GDP Growth Rate	World Bank Governance (Six Elements)	Average	Standard Deviation*
United States	3	1	2.00	1.41
China	1	3	2.00	1.41
Japan	3	1	2.00	1.41
India	1	3	2.00	1.41
Germany	4	1	2.50	2.12
United Kingdom	4	1	2.50	2.12
France	4	1	2.50	2.12
Italy	4	2	3.00	1.41
Russia	1	4	2.50	2.12
Brazil	4	3	3.50	0.71
Canada	3	1	2.00	1.41
Mexico	3	3	3.00	0.00
Spain	3	1	2.00	1.41
South Korea	3	1	2.00	1.41
Indonesia	2	4	3.00	1.41
Australia	3	1	2.00	1.41
Average	**2.88**	**1.94**	2.41	1.46
Standard deviation	**1.09**	**1.18**		

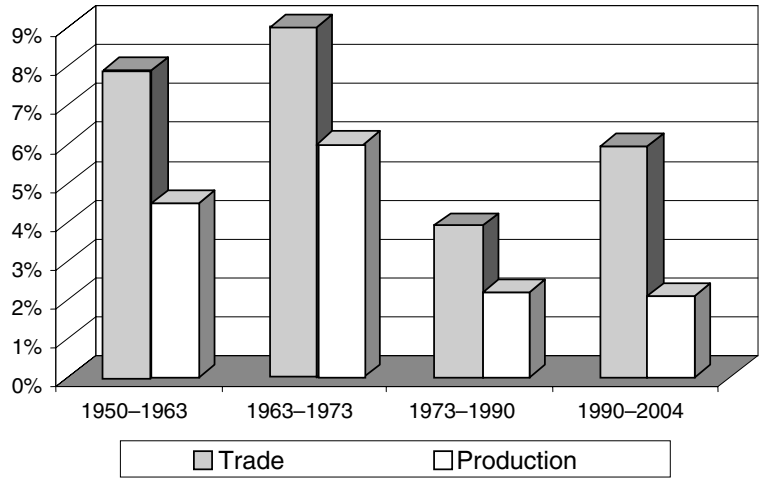
*Standard deviation under 1 suggests a strong correlation.
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (September 2006).

EXHIBIT 1.4 WORLD BANK GOVERNANCE VERSUS GDP GROWTH RATES

tasks, and as an unfair and added cost with few tangible benefits—a necessary evil to doing business. A more sensible approach is to accept improved governance as a strategic imperative and key to the growth and prosperity of all organizations. This entails setting the example at the top of the organization and then having all managers take ownership to the process. Once this occurs, the lower-level activities of risk management and the internal controls to meet laws, regulations, and standards will start to fall into place.

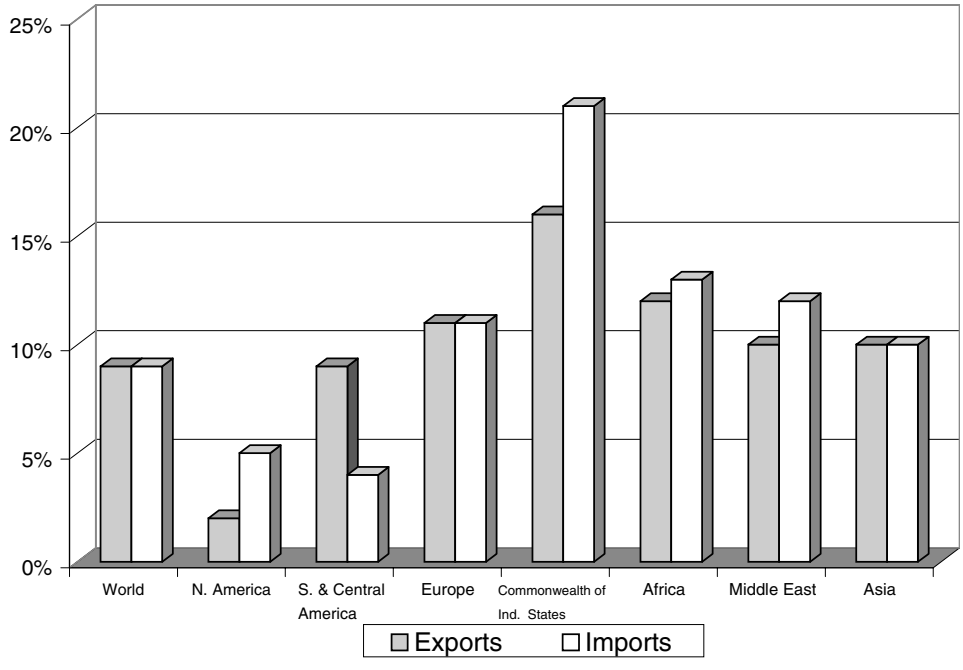
It is natural for companies to complain about the cost of complying with regulations and best practice frameworks. Many of the loudest critics fail to mention that the high costs of compliance are caused by decades of neglect, mergers and acquisitions, and the shortsightedness of their management. The internal control improvements forced by regulations will ultimately make organizations more efficient and therefore more profitable.

Regulators. Regulators have not always done a good job of considering the costs versus benefits of laws and regulations they create and administer. While there are some good efforts underway to harmonize regulations and standards, there are still far too many local variations in place to protect the parochial interests of governments and industries. Protectionist regulations typically fail



Source: World Trade Organization, 2005 International Trade Statistics.

EXHIBIT 1.5 GROWTH IN GLOBAL TRADE VERSUS GLOBAL PRODUCTION



Source: World Trade Organization, 2005 International Trade Statistics.

EXHIBIT 1.6 ANNUAL GROWTH IN TRADE, 2000–2004

and cause more harm than good. The goal should be to create a cross-border level playing field based on best standard frameworks that facilitate economic growth and prosperity. The OECD Principles, the IFRS/global GAAP, and the Kyoto and Basel II accords are all examples of movements in the right direction.

(b) MAP PROCESSES TO CONTROLS TO AUDITED REGULATIONS. Organizations. In order to avoid redundant compliance activities, it is critical to create a matrix that captures the relationships among business processes, the risks associated with processes, the internal controls deployed to mitigate the risks, the tests used to validate the effectiveness of the controls, and finally the regulations to which the internal controls apply. The example of accounts payable illustrates the point.

The accounts payable process covers the activities to pay suppliers for the goods and services they provide a company. One of the many risks associated with the accounts payable process is that a buyer and/or a payables accounting clerk would commit fraud by setting themselves up as a supplier to the company. The control to prevent this is typically known as segregation of duties (SOD). Most financial governance regulations (Sarbanes-Oxley, OECD Principles, Basel II, etc.) contain requirements to prevent violations in segregation of duties. The tests auditors use would include testing access and change controls in the accounts payable application software for the existence of detective and/or preventive controls. By mapping the process, risk, control, audit test, and regulations, an organization can avoid redundant compliance costs by using one control and audit test for multiple regulations. This will also help organizations make the business case for standardizing and automating the control and testing process.

Regulators. Regulators should publish a matrix with the mapping of the common processes that most companies will have to deal with in their compliance activities, including the acceptable tests for each regulation. Regulators should maintain and publish recommended best practices and lessons learned to assist organizations in improving their compliance performance.

(c) RATIONALIZE AND PRIORITIZE RISKS. Organizations. Even the smallest organization can implement a process to rationalize and quantify risks. It can be as simple as creating a scoring system for three or more variables of risk such as economic impact (severity), likeliness of occurrence (frequency), and ability to detect (discovery). Such a system requires a consensus from the audit committee down to the business owners of each organization. Those risks and controls with the highest risk scores would obviously receive the greatest level of effort and should be the first candidates for process and technology improvements.

Regulators. As we discuss in our COSO and operational risk chapters, it is time to revisit the effectiveness of any risk framework that does not provide the means to quantify risks.

(d) INCREASE CONTROLS STANDARDIZATION AND AUTOMATION. Organizations. Manual controls are, by nature, costly and ineffective. Automated controls lower costs and lower risks. Process improvements go hand in hand with automation. It makes little sense to automate inefficient and nonstandardized controls. Auditors will typically want to review manual controls every quarter, because manual controls are only as good as the person handling them. Auditing manual controls is more labor intensive and less effective than auditing automated controls. Automated controls do not have to be overly complex, either. The company can start with a good document and records management system, and then expand to automated work flows to control key business processes that have the greatest impact on financials or the greatest threat of fraud.

Regulators. While regulators and external auditors are not supposed to be technology experts, they need to increase their understanding of the many compliance automation tools that have been available for years. This is not to say that they are advocates for overly complex and expensive technology solutions, but they should be advocates for basic tools that are readily available and affordable in the marketplace. Tools to control document and records management and the audit operations, segregation of duties, financial consolidation, and application controls have been around for some time and will continue to drop in cost. In some cases, regulators and auditors have a conflict of interest in recommending these solutions, in that the tools will reduce the need for audit services. Fully automated controls with remote-view-only access could eventually make much of the on-site audit activity a thing of the past.

(e) CREATE AN INTERNAL CONTROLS GRADING SYSTEM FOR STOCKS. Organizations. Organizations should accept improved internal controls as a strategic competitive advantage and not as simply a cost of doing business. Regardless of the regulatory requirements, improved internal controls are a sound investment that will lower costs and improve decision making.

Regulators. The debate continues as to the cost versus benefits and effectiveness of measures to improve internal controls. Investors do need protection against organizations that lack effective internal controls. In the United States the system is punitive, with material weaknesses charged against wrongdoers but nothing rewarded to those who have excellent internal controls. It is a simple pass/fail system in which there are no tangible rewards for excellence. The same companies that have not undergone expensive internal control assessments are listed alongside those that have failed assessments (material weaknesses or financial restatements) or have not yet taken them at all. In the United States, nonaccelerated and foreign filers were not required to meet Section 404 requirements through 2006. There is no simple means to know the compliance status of a listed company.

A simple internal controls grading system for publicly traded companies may provide at least a partial answer. (We also include this recommendation

in our U.S. corporate governance chapter.) In such a grading system, those companies that have excelled in meeting tough internal controls requirements over an extended period would receive the highest score. Those with internal controls issues would receive lower grades. Smaller or start-up companies would be given the ability to opt out of the process and be given an "X" grade. A company's internal controls grade would appear next to its stock symbol, making it easy for even a casual investor to decide among offerings based on their internal controls scores.

A more complex grading system would require a cross-border consensus around acceptable internal controls standards and frameworks—a commonsense version of Sarbanes-Oxley that quantifies risk and seeks controls for the significant few and not the insignificant many. It would include generic and industry-specific best practice internal controls frameworks. Such a system would also require a consensus around breaches in internal controls, sometimes called material weaknesses. Ideally, all publicly traded companies would be graded on the same basis.

1.8 WHY READ THIS BOOK: THE CASE FOR GOOD GRC

Surveys have indicated for many years that investors will pay a stock premium for companies that are well governed. It makes sense that a lower-risk investment is seen as a safe haven. If the safe haven also has a good track record of stability and profit growth, the premium will increase. The size of the premium is very market dependent, with greater premiums in more poorly governed markets. McKinsey and Company's 2002 survey showed premiums ranging from 11 percent in Canada (the best-governed country, according to our World Bank data) to 40 percent in developing markets.[17] The premiums also wax and wane based on the scandal cycles—typically increasing after investors witness Enron-type collapses, but decreasing during boom times due to short memories.

Well-governed companies have other advantages beyond premium stock prices. They can typically access capital at lower costs than their poorly governed competitors. The major rating agencies (Fitch Ratings Ltd., Moody's Investors Service, and Standard & Poor's) are more focused on good governance, risk, and compliance management in their company assessments. In some industries they are holding companies to higher standards ahead of the regulators. (The impact of rating agencies on operational risk is discussed in two of our chapters: Chapter 14, "Operational Risk Management (ORM) Best Practices," and Chapter 17, "Operational Risk Management in Financial Services.") In the United States, privately held companies thought that they were immune to the Sarbanes-Oxley Act until they found banks and insurers looking for them to meet the higher standards in order to receive the most competitive rates of financing and insurance.

Well-governed companies will typically attract and retain higher-level talent. Employees would rather brag to their family and friends about the good deeds and reputations of their employers than apologize about their publicly embarrassing misdeeds and failures.

Some of the benefits of good governance are:

- Greater access to capital markets
- Lower cost of capital
- Ability to attract and retain higher-caliber talent
- Higher-quality and more timely decision making
- Greater ability to respond to and recover from crises and disasters
- Improved operational efficiency and lower operating costs
- Fewer conflicts and lower stress levels
- Improved community and industry reputation

1.9 ORGANIZATION OF THE HANDBOOK

Corporate Governance. Part One provides high-level overviews of corporate governance. It includes an evaluation of the effectiveness of the COSO framework, corporate tax problems caused by the dual book system, the importance of the internal audit function, the need to control outsourced processes, the importance of consolidation and reconciling financial statements as part of the period end process, and the issues around stock options. Part One concludes with two chapters on fraud and corruption—an introduction to the subject and the means to fight the problem.

IT Governance. Part Two provides high-level overviews into information technology governance, including a general discussion about IT governance, the International Standards Organization (ISO) standards impacting IT, and the role of Control Objectives for Information Technology (CobiT).

Operational Risk. Part Three provides four chapters on operational risk. It begins with an introduction to best practices in operational risk management, followed by discussions of six sigma as a good practice to control operational risk, quantitative tools that can be deployed to control operational risk, and measuring the effectiveness of operational risk programs.

Technology and Tools. Part Four provides a survey of the technology and software tools available to improve governance, risk management, and internal controls. It includes the following tools: enterprise search and automated testing, audit operations applications, segregation of duties, database management, and product life cycle management (PLM). It concludes with an introduction to eXtensible Business Reporting Language (XBRL).

Environmental Governance. Part Five provides national, regional, and material environmental guidance, with chapters covering materials (e.g., the European Union's Reduction of Hazardous Substances/Waste Electrical and Electronics Equipment directives), China, the European Union, India, Latin America, and the United States.

Industry Governance. Part Six covers a variety of industries that have unique governance requirements, including electronics (homologation), Internet

commerce (privacy versus security), logistics, transportation, pharmaceuticals, the public/government sector, retail, supply chain, and telecommunications.

Financial Services Governance. Part Seven covers the unique challenges facing the financial services industry with chapters on insurance, Islamic finance, operational risk in banking.

Regional and National Guidance. Our final section provides high-level introductions to corporate governance in the top 16 GDP nations, capturing 75 percent of global GDP as measured by purchasing power parity (PPP); Islamic nations; and the regions of Africa, Latin America, Southeast Asia, and the European Union.

Supplemental Chapters. We have also included a web link to six supplemental chapters and case studies: banking in China, Malaysian insurance, South African banking, bad behavior in Australian banking, and measuring effectiveness and performance of GRC in the United States.

Notes

1. Stewart Kyd, "A Treatise on the Law of Corporations," 1794, 13.
2. Wikipedia, "The Corporation," http://en.wikipedia.org/wiki/Corporation.
3. Mervyn K. Lewis, "Islamic Corporate Governance," International Association for Islamic Economics, *Review of Islamic Economics* 9, no. 1 (2005): 5–29.
4. Ibid.
5. Margit Osterloh and Bruno S. Fry, "Corporate Governance for Crooks? The Case for Corporate Virtue" (Working Paper 2005-10), www.Crema-research.ch.
6. Ibid., 17.
7. Ibid., 2.
8. Ibid., 15–16.
9. Timothy Curry and Lynn Shibut, "The Cost of the Savings and Loan Crisis: Truth and Consequences," *FDIC Banking Review* (1999).
10. See COSO's Executive Summary, "Enterprise Risk Management—Integrated Framework," September 2004.
11. See the National Institute of Standards and Technology (NIST), Special Publication 800-30, "Risk Management Guide for Information Technology Systems," July 2002.
12. "The Private Equity CEO," *Wall Street Journal*, November 6, 2006, B1.
13. John Hawksworth, head of macroeconomics, PricewaterhouseCoopers, "The World in 2050: How Big Will the Major Emerging Market Economies Get and How Can the OECD Compete?," March 2006.
14. Harvey L. Pitt, "Globalization of Capital Markets: On the Road to Global Governance Standards," *Compliance Week*, May 31, 2006.
15. Ibid.
16. Greg Ip, Kara Scannell, and Deborah Solomon, "Trade Winds: In Call to Deregulate Business, a Global Twist; Onerous Rules Hurt U.S. Stock Markets, But So Do New Rivals," *Wall Street Journal*, January 25, 2007, A1.
17. McKinsey and Company, "Global Investor Opinion Survey," 2000 and 2002.

PART 1

CORPORATE GOVERNANCE

CHAPTER 2

A RISK-BASED APPROACH TO ASSESS INTERNAL CONTROL OVER FINANCIAL REPORTING (ICFR)

Tim J. Leech, FCA·CIA·IT, CFE, CCSA
Jeffrey C. Thomson, MS

Note: This guide is a condensed version of a more comprehensive Institute of Management Accountants (IMA) discussion paper titled ''A Global Perspective on Assessing Internal Control over Financial Reporting'' circulated for comment globally and filed with the SEC in September 2006. The full text can be found at www.imanet.org/pdf/IMAmanagementguidancetoSEC906.pdf.

2.1 A RISK-BASED APPROACH TO ASSESSING ICFR

(a) INTRODUCTION. The Security and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) in the United States have repeatedly stressed that companies should apply a top-down/risk-based approach to assessing Internal Control Over Financial Reporting (ICFR) for Sarbanes-Oxley (SOX) Section 404. An Institute of Management Accountants (IMA) research project completed in 2006 titled COSO (Committee of Sponsoring Organizations) 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices indicated that SEC registrants, their advisers, and auditors have widely divergent views on how to actually complete a top-down/risk-based review of ICFR. This disparity of definition and application of "risk-based" was confirmed in numerous comment letters sent to the SEC and PCAOB in response to their December 2006 exposure drafts relating to management and auditor assessments of ICFR for SOX.

To provide a solid basis for discussion on this topic, the IMA drafted and exposed for comment a paper titled "A Global Perspective on Assessing Internal Control over Financial Reporting." This guide is a condensed version of that discussion paper that describes a step-by-step approach to assess ICFR that conforms to international risk management standards. Exhibit 2.1 contains a basic flowchart which summarizes the key steps in the risk-based approach described in this guide.

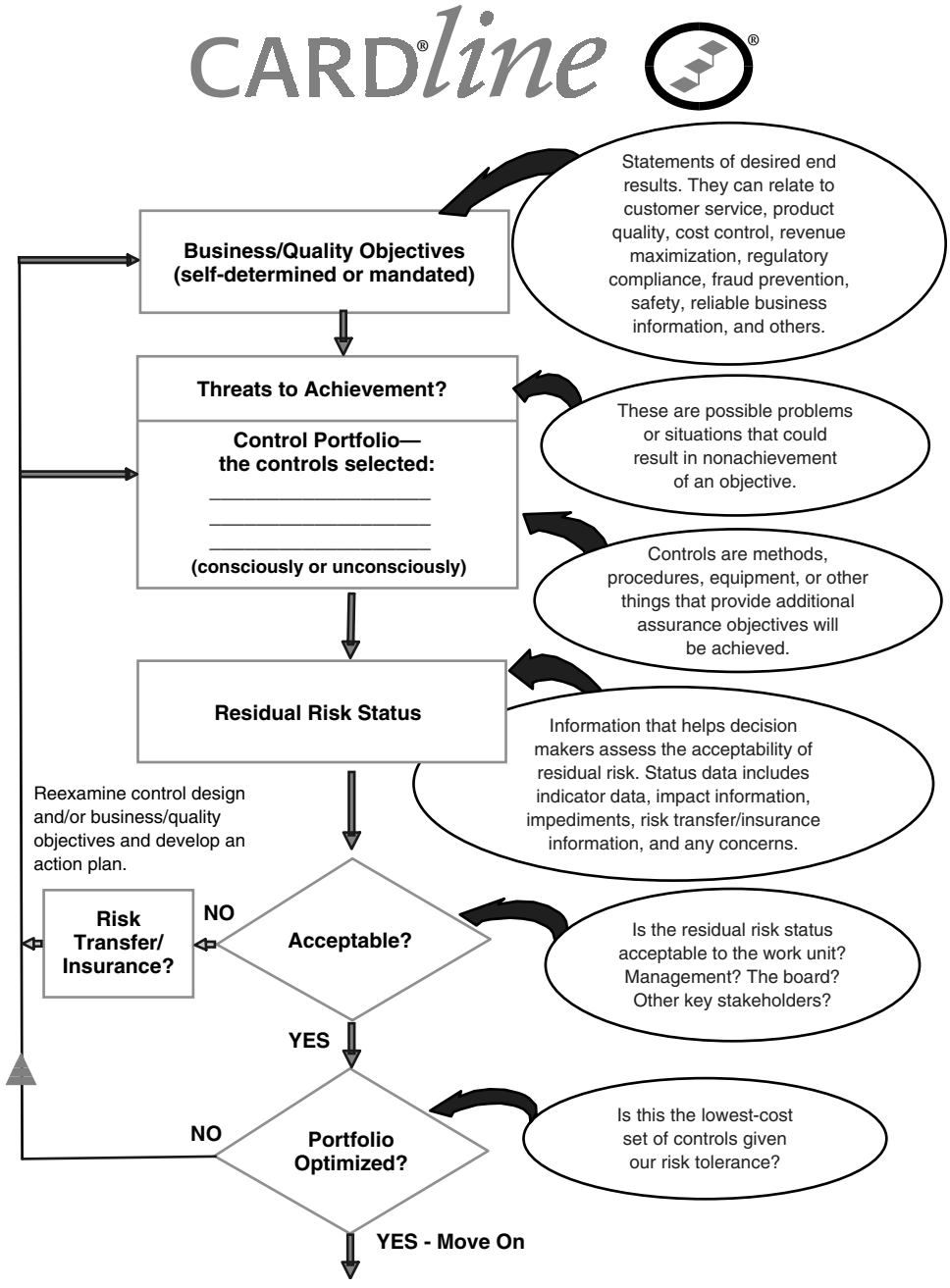
2.2 DETERMINE KEY STAKEHOLDERS

When trying to solve a perceived problem, it is important to take the time to identify and prioritize the key stakeholders that have a direct and indirect stake in solving it. The focus of the authors of the Sarbanes-Oxley Act of 2002 was clearly on investor protection. The stated purpose of SOX is:

> To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes.

All security regulators around the world that want to ensure the fairness and attractiveness of their capital markets share this goal. To date, only a few securities regulators have decided, at least at this point in time, that the frequency and magnitude of unreliable reporting is a big enough problem to their economies to warrant following the approach implemented to date in the United States.

In addition to capital market investors, venture capitalists, banks and other lenders, credit rating agencies, employees, pensioners, suppliers, customers, and many others rely to varying degrees on information contained in external financial disclosures. In addition to these parties, the senior management team of all organizations should care whether their internal accounting processes are producing reliable information for investors externally and for resource allocations and strategic decision making internally.



Source: © 2007 Institute of Management Accountants.

EXHIBIT 2.1 KEY STEPS IN RISK-BASED APPROACH

2.3 ESTABLISH THE RISK MANAGEMENT CONTEXT

(a) GENERAL. Agreeing that public companies should publish reliable financial disclosures is relatively easy. Agreeing on just how reliable/error free the disclosures need to be and, most important, the consequences if they are not reliable is far from easy. The fact that management's motivation, remuneration, goals, and aspirations can sometimes conflict with the needs of other stakeholders, at least in the short term, further complicates the issue. Simply defined, establishing the risk management context means understanding the internal and external environment and the reasons why the primary overarching risk that auditor-certified financial statements contain material errors should be mitigated. Understanding the interface between management's perspectives and motivations and those of regulators and outsiders, particularly the tolerance of both groups to the existence and/or potential of undetected errors in public disclosures, is particularly important. It also means seeking agreement on how reliable or, stated another way, how unreliable/inaccurate financial statements can be and still meet the needs of relevant stakeholders. This information has major cost implications.

(b) RISK CRITERIA—BIG PICTURE CORPORATE LEVEL. A primary goal of securities regulators is that public companies produce timely and reliable financial disclosures. The term *risk criteria* is defined in the AS/NZ 4360 Risk Management standard and the Internal Standards Organization (ISO) Guide 73, *Risk Management Vocabulary—Guidelines for Use in Standards*, as "the terms of reference by which the significance of risk is assessed." In this discussion draft, the key macro-level risk is that the financial statements are not reliable or, stated another way, auditor-certified financial statements contain undetected material errors in account balances and/or note disclosures.

There are eight important risk criteria at the big picture corporate level:

1. *Implications to the company's credit rating.* All of the major credit rating agencies have published papers in more or less detail on their attitude to control weaknesses disclosed under the current U.S. SOX regime. What they have not stated is how they obtain similar information in countries that do not require management and/or auditors to make specific representations on ICFR effectiveness, disclose material weaknesses in ICFR, or state the amount of rework of the accounts generated by the external audit. It is clear that the credit rating agencies do consider the track record of companies that have had to issue restatements of their financial statements and the reasons why these situations have occurred. One credit rating company, Moody's, has gone so far as to categorize SOX material control weaknesses as "Category A" and "Category B" issues. When a Moody's Category A control weakness is disclosed, Moody's has stated that it isn't particularly concerned because it believes that external auditors can effectively "audit around" the problem. However, when what Moody's calls a

Category B control weaknesses is disclosed they consider these situations to be serious because they "question the ability of the auditor to effectively 'audit around' a Category B weakness."

2. *Implications to the company's reputation.* Companies are increasingly concerned about whether the market views their financial disclosures with some significant level of distrust and/or disbelief. When this situation occurs, it reflects badly on the issuing company's senior management and board, as well as the external auditor that certifies the company's financial statements.
3. *Implications to the company's cost of capital.* The trust and reliance that lenders place in management and management representations and the risk premium lenders assign to an organization are often linked to the company's track record of issuing reliable audited financial statements. There is preliminary evidence that at least some lenders are starting to take an interest in information on ICFR, but it is also likely fair to say that lenders have not shown high levels of interest in the current state of a company's ICFR. It is important to note, however, that the attitude of credit rating agencies does directly impact on the views and decisions of lenders and investors.
4. *Personal implications to senior executives and board members.* The United States has shown the most zeal so far in punishing executives who have knowingly and/or negligently allowed their companies to issue false or misleading financial statements. The evidence in the United States is seen in the jail sentences being handed down, corporate and personal fines being levied, the legal threat of requiring bonuses to be forfeited, civil actions being launched, and more. The attitudes of the boards of directors of U.S. listed companies toward unreliable financial statements have been variable. Regulators in countries other than the United States have generally not shown the same level of focus in this area. It is important to note that at least some companies that have a track record of unreliable external disclosures are experiencing difficulty attracting high-caliber senior executives and board members, particularly CFOs and audit committee members, and having to increasingly pay a premium to attract them because of the potential personal implications.
5. *Audit firm resignations/refusals.* A number of public companies have, for all intents and purposes, been black-listed by the big four accounting firms, which have resigned or refused their business because the integrity and/or reliability of their accounting controls is questionable. These companies must resort to using lower-tier audit firms willing to accept their business that have higher risk tolerances for their audit opinions. Situations like this can, in turn, impact credit ratings, cost of capital, and share price.
6. *Impact on the company's share price.* Research in this area is still at a very early stage with somewhat inconsistent results. To date, the only country

that has mandated public disclosure of the specifics of material weaknesses in ICFR detected by management or auditors is the United States. It isn't at all clear at this point that investors are discounting the price of shares in companies listed in countries that do not require disclosure of the type of information on ICFR currently mandated in the United States, and there is at least some evidence that absence of information on ICFR has no impact or very limited impact on share price. A May 2006 comment paper issued by the Fédération des Experts Comptables Européens on the topic of management reporting on ICFR reports, "There is no evidence of demand for public reports on effectiveness of internal control in Europe" (Section 2, General Comments). This is an area that warrants considerable research to determine how markets react to the absence of information on ICFR from management and/or external auditors.

7. *Personal philosophy of the company's CEO, CFO, and board of directors.* The tone at the top is regularly cited as key to the issue of reliable external disclosures. The general tolerance of CEOs, CFOs, and boards of directors to unreliable external disclosures and the way they personally react when evidence emerges to the contrary are key risk criteria in this area. It is important to note that even companies with excellent tone at the top can suffer instances of materially wrong financial statements because of the inherent limitations of internal control and the fact that some level of risk must be accepted to make a profit and stay in business.
8. *Likelihood external auditor opinion on financial statements is wrong.* There is a strong implicit assumption in the current U.S. SOX rules that external auditors will render less incorrect audit opinions when they are equipped with better information on the state of ICFR. This would imply that external auditors should, on balance, have a higher audit opinion failure rate in countries that have not endorsed SOX-like rules related to ICFR. This is a major consideration in the debate over the cost/benefit of the SOX regulatory regime in the United States that warrants serious research to prove or refute the assumption.

(c) RISK CRITERIA—SUBSIDIARY LEVEL. A large percentage of companies, even smaller public companies, have one or more subsidiaries that are consolidated to form the financial disclosures filed with securities regulators. The degree of autonomy and the reporting lines of the personnel responsible for accounts and financial statements of these companies can vary widely. Two of the key risk criteria that impact attitudes of executives in subsidiaries are:

1. *Importance attached to reliable financial statements and accounts by the head office*. The overall attitude toward undetected errors in accounts at the subsidiary level is communicated in a number of important ways. This includes the importance to reliable accounts and effective ICFR in job

descriptions, the link of reliable accounts and ICFR to compensation/reward/punishment systems, the rigor of analysis and questions posed by the head office consolidation team to the accounting personnel in subsidiaries, the interest of the head office in the frequency and magnitude of errors detected by the external auditors in the course of their audits, the existence and competency of any internal audit function that exists, and others.

2. *Personal implications to controllership and local operating management* in terms of bonuses and promotions when conscious and/or negligent errors in the accounts filed with head office are identified.

(d) RISK CRITERIA—ACCOUNT/NOTE DISCLOSURE LEVEL. Although the risk criteria that exist at the corporate and subsidiary levels play major roles influencing behavior of senior controllership staff and form the macro-level risk context for decision making, the risk criteria related to the individual accounts and notes that comprise the financial statements at the subsidiary and corporate levels are also important. These risk criteria impact on the attitudes of the staff that impact directly or indirectly on the reliability of specific accounts and/or note disclosures. The same basic elements listed earlier influence the perception of accounting staff regarding the importance or reliable financial disclosures.

2.4 RISK RATING AND RISK IDENTIFICATION

When tackling the task of applying a true top-down/risk-based approach to assessing ICFR, assurance contexts to be assessed must be established at multiple levels and risk rated before deciding where to invest the time and resources required to complete more detailed formal risk/control assessments.

As stated throughout this paper, the most important macro-level assurance context for ICFR is to ensure that auditor-certified financial statements, including the notes, are reliable.

This broad macro-level assurance context should constitute the starting point for an entity's macro-level risk/control assessment. This section provides our specific views on how top-down/risk-based ICFR assessments should be defined for companies of all sizes to realize the value in their compliance programs.

Since companies often have multiple subsidiaries and locations, hundreds, if not thousands and even tens of thousands of individual account balances, and scores of note disclosures, a universe of ICFR assurance contexts cascading from the macro-level context must be identified, risk rated, and the conclusions reached and documented for possible review by independent quality assurance staff. For U.S. listed companies, the primary independent quality assurance agent for ICFR is the external auditor. In larger companies the company's internal audit department and/or a SOX quality assurance team may also play important roles.

(a) RISK RATING ASSURANCE CONTEXTS FOR ICFR. A key step before embarking on more detailed granular risk/control assessments is to identify and risk

rate the individual assurance contexts that support the macro assurance context at the corporate, subsidiary, and account/note levels. A sample of 14 risk rating criteria that can be used when arriving at a composite risk rating on each of the assurance contexts that support the macro-level or parent assurance context includes:

1. Detected error history—external auditor
2. Detected error history—detected by management after release of statements
3. Detected error history—detected by management prior to release of statements
4. Complexity of accounting
5. Absolute dollar/unit of local currency value/impact of location/account
6. Detected error history—regulators/tax authorities/customers/others
7. Detected error history—internal audit
8. Detected/known errors in other companies in the same business sector
9. Amount of management judgment/subjectivity
10. Importance of account/location to security analysts
11. Importance of account/note disclosure to debt covenants
12. Susceptibility of account to fraud from insiders
13. Susceptibility of account to fraud from outsiders
14. Account/note linkage to the company's reward/compensation system

This is an area where additional research would help refine the accounts/areas in a company that would most benefit from more rigorous and formal risk and control assessment. Some companies have gone so far as to develop weighted numeric risk scoring systems that are then applied to their universe of ICFR assurance contexts to decide the frequency and extent of analysis and testing each assurance context will receive. The more these ratings are based on facts as opposed to unsupported guesses and subjective views, the better this system will work to actually ensure that formal assurance resources are focused where they are most needed. The ratings assigned at this stage have massive and ongoing cost implications because they should, if regulators allow it, influence the extent of risk/control design and control confirmation/operating effectiveness assessments going forward (i.e., the higher the risk rating, the higher the assurance cost annuity). If the risk rating system is reliable, it should allow for reduced risk and control assessment documentation and testing in areas that have low overall risk scores. These scores should be adjusted on an ongoing, real-time basis as new information emerges or, at a minimum, reassessed annually. Again, the goal is *not* to produce a one-size-fits-all prescription; rather, the goal is to suggest a system that can replace subjective ratings systems that are largely based on the absolute dollar size of account balances.

(b) IDENTIFYING RISKS TO ASSURANCE CONTEXTS SELECTED FOR ADDITIONAL ANALYSIS. Once the assurance contexts to be assessed have been

agreed on and risk rated, the next step, using the terminology in the AS/NZ Risk Management standard, for assurance contexts selected for additional formal assessment, is risk identification—"the process of determining what, where, when, why, and how something could happen." As a general statement, this involves identifying, understanding, and documenting a list of real or potential situations at the big picture company level that could cause the nonachievement of the assurance context being assessed. This list should be comprehensive enough that it covers plausible risk scenarios, but not include far-fetched risk scenarios. A cardinal rule in risk-based assessments is "Miss the risk, and risk blowing the assessment."

Techniques to build a reasonable list of plausible risks for an entity-level risk assessment for ICFR and for more granular subelements include:

- *Research and observation.* Simply explained, this requires identification of actual situations that have already occurred in other similar public companies that resulted in materially incorrect financial disclosures. Reading newspapers, magazines, and journals like *BusinessWeek* and *Compliance Week* can produce a solid starting point. A number of relevant web sites such as Audit Analytics (www.auditanalytics.com) that track all public companies that have had material control weaknesses and/or restatements of their financial statements are available to assist with this activity. The most dominant risk at the entity level that has emerged from recent scandals is when a "CEO/CFO/senior executive instructs or otherwise influences staff to make entries that are fraudulent." Although this may seem to be a somewhat blunt assessment approach, there is no point denying that it was specifically this risk that resulted in SOX being enacted by the U.S. Congress. Other common risks include "Compensation system, particularly the company's stock option plan, tempts senior-level staff to falsify earnings," "CFO and/or accounting support staff are not current on GAAP," "Staff members lack adequate knowledge of applicable federal/state tax law," "There is lack of rule clarity on how to deal with certain transactions/situations," and others. Every major financial statement misstatement that has been detected around the world, including Enron, WorldCom, HealthSouth, Parmalat, Nortel, and hundreds of others, has a cause of failure.
- *Company-specific history.* As companies mature, a large number of them, as a result of internal analysis, the work of their external auditor, and the passage of time, realize that they have publicly issued financial statements that were materially wrong in one or more respects. Few companies in the world have continuously produced fault-free disclosures prior to the audit/inspection process of their external auditors. Sometimes these situations result in public restatements, while in other situations there is only the existence of internal knowledge on the part of one or more employees that

one or more components of the publicly released financial statements were not, in fact, reliable. If these situations are analyzed and a cause of failure determined, it is generally easy to determine the key risks that caused the undetected error. For companies that, for whatever reason, place high reliance on the end-of-the-line inspection ability of their external auditors, a key risk is always that "The external audit team assigned doesn't detect and/or require correction of errors that exist in the accounts." Again, the quality mantra of "building quality in, not on" (after-the-fact inspection) is critical, in our view, to the goal of cost-effective assessments.

- *Experience of senior-level staff.* One of the advantages of growing older and gaining decades of experience in the accounting and control field, often in multiple companies, is that a person gains a broad experience base of what can go wrong and result in major errors in the accounts. This experience base can be used to identify plausible, company-specific situations that have the potential to result in material errors in the financial statements.
- *Industry-specific scenario analysis.* This is a technique that can draw on information from the preceding three methods for inspiration, or be done using pure imagination of consultants and/or staff to produce plausible scenarios that the controls currently in use would not mitigate. The current reforms in the banking sector mandated by Basel II require that all major banks in the world demonstrate that they are regularly doing scenario analysis on the full range of operational risks, including those related to reliable financial statements. This technique is one that can help detect and prevent the next big disclosure disaster that has not happened yet elsewhere (e.g., the use of special-purpose vehicles at Enron).
- *Risk source analysis.* This technique uses a list of potential sources of risk to trigger ideas on possible scenarios that would cause a company's financial statements to be wrong. An example of one risk source framework that can be used is the CARD®*menu* shown later in the chapter. When using aids like risk source lists, the general rule is they should be as granular as is necessary to pick up the significant risks. A risk source list that contains 100 risk sources may not be as effective as one that is more summarized but still causes the assessors to identify a good list of significant risks. The example in this paper demonstrates a risk source framework that has a fairly limited number of risk source categories but has proven very effective as a risk identification tool.
- *Industry checklists.* Although it is generally better to rely on the methods listed to generate an industry-specific/company-specific set of risks, regulators have typically been willing to accept the use of so-called canned risk and/or control assessment checklists provided by consultants, external auditors, or other providers. When such aids are used, care should be taken to try to validate that these assessment aids do, in fact, result in identification of the most probable company/industry-specific risks to

reliable financial disclosures. When canned checklists have been employed and produce a conclusion that controls are effective, it is very important to monitor whether management and/or the company's external auditors are still finding material errors in the draft financial statements. When external auditors find material errors after management and the external audit team have concluded controls are effective, it is at least prima facie evidence that the assessment aid and/or current risk assessment process is inadequate.

A top-down approach that starts with a macro-level assessment on the assurance context of ensuring reliable auditor-certified financial statements will often identify where the major holes in a company's ICFR system are without the high expense and massive amount of time required to complete what many refer to as the bottom-up approach to assessing ICFR. A bottom-up approach starts by documenting and assessing all the accounting processes that generate or support debits and credits regarded as material in the general ledger. More than a few companies in the first round of SOX did not start at the macro-level assurance contexts and did not identify and document the truly key risks that history tells us have regularly led to material financial statement errors and the mitigating controls in place to prevent them.

In addition to the type of top-down/entity-level assessment described that starts with the macro-level assurance context of ensuring reliable auditor-certified financial statements, the process of identifying risks for the more granular assurance contexts that must be assessed to arrive at a supportable conclusion on ICFR must also be done.

2.5 ANALYZE AND EVALUATE RISKS

Once the assurance context universe has been risk rated and plausible risks to the ICFR assurance contexts selected for analysis have been identified and documented, the next step is to analyze and evaluate the specific risks. In cases where history clearly indicates a track record of internally or externally detected material accounting errors at the corporate level or in specific company locations, subsidiaries, departments, and/or accounts and notes, this information needs to be carefully assessed and the relevant risks associated with the errors isolated for special assessment and evaluation treatment.

The process of analyzing risks includes assigning likelihood and consequence ratings to each risk. Generally an attempt should be made to produce these ratings before considering controls (inherent or gross risk ratings). Estimates can also be assigned for the net or residual risk that remains after considering controls, although this is often difficult and costly if it is done using facts as opposed to purely subjective opinions.

Great care must be taken that the risk analysis process does not become too granular and costly and become an industry in itself. The endgame is to decide which risks are not currently sufficiently mitigated given the organization's

tolerance to accounting misstatements (i.e., these are often identified as "red-rated" risks). In real life, people and companies frequently use an experiential, iterative approach that causes them to modify their controls after they are presented with tangible evidence that contradicts previously held views of the likelihood or consequence of a risk (e.g., the risk that staff might forge signatures on sales contracts to earn a bonus in a quarter or fiscal year-end gets mitigated after a major scandal where this occurs emerges). Using the risk identification techniques outlined in this chapter will help by generating risks that have already proven to be plausible and have, in fact, already resulted in material undetected errors in other public companies. In order to dismiss such risks as irrelevant, a company should be able to explain why its controls would mitigate the risk or be willing to state that its current controls might not mitigate the risk and it accepts the consequences.

2.6 TREAT/MITIGATE RISKS

(a) TREAT RISKS USING COSO 1992 CONTROL CRITERIA

(i) Using COSO 1992 for Control Criteria Centric Assessments. To comply with the requirement in current SOX regulations that assessments be done in accordance with a suitable control framework, some companies annually, and sometimes even quarterly, have been completing a high-level size-up of how their current controls compare to the type of control criteria described in COSO 1992. This approach is sometimes called the "control criteria centric" approach, and it is done without explicit and direct reference to specific risks that threaten the macro-level objective of reliable financial statements. This approach involves taking the five primary COSO 1992 categories and subelements that comprise the categories and attempting to determine on a binary basis whether the company currently demonstrates achievement of the COSO 1992 control elements for ICFR.

To date few, if any, companies have publicly reported material control weaknesses in their controls relative to any specific COSO control categories or subelements. The major challenge when attempting to use the COSO 1992 framework this way is that it was not written with the intent that it would ever be used for pass/fail assessments on a specific company's ICFR effectiveness. The Malcolm Baldrige quality system in the United States administered by the American Society for Quality (one of the participating reviewers of this document) is an example of a framework that has been specifically developed to generate repeatable numeric assessments against the quality system evaluation criteria contained in the framework. It is important to note that the Baldrige framework does not define what a passing grade should be with respect to a company's quality management system; rather, in the spirit of continuous improvement, it defines quantitatively an organization's progress toward global benchmarks in various categories—categories that are refined and updated for relevance and predictability each year by Baldrige system administrators.

Whether a control criteria centric assessment approach that attempts to determine the degree to which a company conforms to control elements in COSO

1992 is what the SEC has in mind when it used the term "top-down" assessment is not known as of the date of issue of this discussion paper. It is not an approach that is currently mandated in PCAOB AS2. It is also not a risk-based approach (it is control criteria centric), but does reflect a top-down emphasis. This issue may be clarified in the new guidance for management.

(ii) Using COSO 1992 for Risk-Based ICFR Assessments. For companies using the COSO 1992 control framework as an assessment aid for a risk-based ICFR assessment approach, the following steps are recommended:

1. *Develop a universe of ICFR assurance contexts* that starts with the macro-level assurance context of ensuring that auditor-certified financial statements are reliable at the corporate level, and then moving downward (i.e., top-down per the SEC) to include a macro-level assessment in all significant subsidiaries that issue stand-alone financial statements, and on to defining assurance contexts for each of the line items and notes in external financial disclosures. The high-level summaries line items in financial statements will then have to be further subdivided to include assurance contexts for all significant general ledger (GL) accounts that comprise the financial statement line items. When grappling with what is a significant GL account or note, the overriding decision criteria are encapsulated in the following question: Would a material error in the assurance context being rated result in stakeholders doing something they wouldn't have done had they known the truth? Additional assurance contexts will be required for reliability of information technology (IT) general controls and can optionally be done separately for the assurance context of preventing fraud-related financial statement misstatement, although the fraud-related risk component can and should be addressed as an integrated element of the assessment done on all assurance contexts, including IT general controls.
2. *Develop and apply a system to risk rate each of the subcomponent assurance contexts identified.* This step allows some percentage of the assurance context universe to be eliminated completely for additional formal assessment based on the risk rating generated or identified for reduced scrutiny. If the type of criteria proposed in this paper are used, even large account balances may be eliminated if they have been error free (both internal and external) and have not been elevated based on other rating criteria such as vulnerability to fraud or industry analyst or debt covenant importance. Companies should agree to the assurance context scoring system they develop with their external auditors, and local regulators may also provide input or even specific rules that must be followed. How far down from the top-level assurance context of assessing risks to reliable auditor-certified financial statements companies must go and be able to prove to outsiders that they have completed formal risk/control assessments is a decision on which senior management, security regulators, and

external auditor standard setters should provide guidance, because it has significant cost implications. Although completing a robust risk assessment on the macro-level assurance contexts of reliable auditor-certified financial statements may provide 80 or 90 percent coverage of the major risks that have caused the types of major problems that led to SOX in the United States, this may not be acceptable to one or more of the key players that input to the assurance context coverage decision, especially U.S. securities regulators and auditor oversight bodies. It is important to note that even 100 percent coverage of the assurance context universe, including formal risk/control assessments on every account in the general ledger, will not provide 100 percent assurance that all significant residual risks that could lead to materially incorrect financial statements have been identified.

3. *Identify and analyze risks that threaten the assurance contexts selected for formal review.* For assurance contexts selected for additional formalized risk/control assessment using one or more of the type of risk identification methods outlined in this chapter, identify relevant risks and evaluate the risks identified in terms of likelihood and consequence. A five-level numeric likelihood/consequence rating system is recommended to provide adequate but not excessive granularity. The key is to find a way to rank risks identified in terms of their likely impact on the assurance context. (See Exhibit 2.2.) Risks can be further analyzed in terms of risk source category, the availability and extent of statistical information available on likelihood and/or consequence of major risks, and other criteria. A major trend currently in the risk management field is to supplement subjective judgments on likelihood and consequence with facts and statistics whenever possible. A table with one of the more common systems used to assign risk levels based on various combinations of risk likelihood and consequence is shown in Exhibit 2.2 and illustrates the concept. Companies can alter the terminology used for likelihood and consequence or

	Consequences				
Likelihood	**Extreme**	**Very High**	**Medium**	**Low**	**Negligible**
Almost certain	Severe	Severe	High	Major	Significant
Likely	Severe	High	Major	Significant	Moderate
Moderate	High	Major	Significant	Moderate	Low
Unlikely	Major	Significant	Moderate	Low	Trivial
Rare	Significant	Moderate	Low	Trivial	Trivial

Source: Guidelines for Managing Risk in the Australian Public Sector, #22 October 1996.

EXHIBIT 2.2 LIKELIHOOD AND CONSEQUENCES

substitute simple numeric scores for the likelihood and consequence levels (e.g., 1 to 5), but should maintain the core principle of demonstrating that a reasonable attempt has been made to prioritize the set of risks identified. The main goal of this exercise is to attempt to sort risks in terms of relevance and potential impact to the ICFR assurance context being assessed.

4. *Identify important controls that mitigate risks with assessable risk levels*. Using the COSO 1992 control framework and the supporting COSO volumes that provide more details on the elements of each control category, identify, document, and categorize important controls in place that mitigate the risks that have been assigned higher-level risk level ratings. (*Note:* The risk level is the result of various combinations of likelihood and consequence.) How far down the list of risks identified that matching is done has significant cost implications. Other COSO 1992 control subelement interpretations or lists have been developed by companies, external auditing firms, and consulting firms; however, it is important to note that the five-member COSO Committee has not formally endorsed any of the many summarized interpretations of the 1992 framework that have emerged over the past 14 years, with the exception of its own 2006 COSO Guidance for Smaller Public Companies (SPC) that defines 20 principles and subattributes. The view may be that as long as the approach is "COSO linked" and companies attest in writing that they are ultimately using the core principles in COSO 1992, the use of "COSO 1992 interpretations" is acceptable to the SEC. Further clarification on this point in the upcoming SEC Assessment Guidance for Management would be useful.

   Mitigating controls identified for the higher-level risks should be categorized to indicate the applicable COSO 1992 control category. This step helps support CEO/CFO representations that an ICFR assessment has been done in accordance with a suitable control framework when national regulators require this representation to be made. This is also a key step to support the need of U.S. listed companies to prove that an attempt has been made to aggregate control deficiencies to determine if, collectively, they constitute a reportable control deficiency. If the areas where deficient controls are identified *often* link to a specific COSO 1992 control category, it may result in concluding that controls are not effective in accordance with that category of COSO 1992. To date, no guidance has been issued by regulators on the subject of how to do a control deficiency aggregation test related to a control model such as COSO 1992, and PCAOB AS2 provides no specific guidance for auditors on this issue. It is important to note that low-likelihood/massive-consequence risks should not be ignored, since many of the major instances of false or misleading auditor-certified financial statements would fall into this category.

5. *Determine whether controls described in step 4 are, in fact, being done as described*. The primary goal of this step is to confirm that controls that have been identified during the risk and control documentation step as mitigators to specific risks are, in fact, being done as described. A simple step that is sometimes overlooked, resulting in significant unnecessary costs, is to simply ask the person or persons most directly responsible for the control whether the control has been done as described during the period being reviewed. In cases where the control owner or sponsor indicates the control was done as described, there may be a need, depending on the level of assurance required, to have one or more independent groups verify that the employees with direct responsibility for the control are telling the truth. This step is sometimes called: independently verifying operating effectiveness, or simply control confirmation.

A simple example of the process of identifying a macro-level risk during a top-down assessment and identifying related mitigating controls would be:

RISK

Senior management (CEO and/or CFO) overrides controls and improperly manipulates/falsifies financial statements.

Risk level rating assigned by management: significant (i.e., extreme consequence combined with a moderate likelihood).

(*Note:* The company's external auditor might have a very different view on likelihood based on past behavior of management related to earnings management.)

MITIGATING CONTROLS

CEO/CFO hiring practices—COSO category: Control Environment

Audit committee oversight—COSO category: Control Environment

Confidential concerns reporting line—COSO category: Information and Communication

Internal audit—COSO category: Monitoring

External auditor audit of financial statements—COSO category: Monitoring

If the goal is to identify only one or two of the controls as a key control to limit the amount of regulatory-imposed management and auditor-control testing, this is a very difficult and subjective decision. In the United States, the likely key control candidates would be audit committee oversight and confidential concerns reporting mechanism (the company's hotline), because the U.S. rules do not allow management to view the external audit as a control. In other countries that do not require management reporting on ICFR and are still tolerant of material undisclosed levels of financial statement adjustments as a result of the work of the external auditor, the key control currently for this particular risk is probably the external audit of the financial statements and the quality of audit staff assigned to do the audit.

Steps would also have to be taken to determine that the controls documented actually were done/completed as described.

The controls currently in use result in some level of effectiveness relative to the assurance context being assessed. Methods to identify the current residual risk status being produced by the controls in place for any given assurance context are outlined later in the chapter. We view the step of identifying and evaluating residual risk status as significantly more important than massive amounts of independent control verification and testing.

(b) TREAT RISKS USING CARD®*MODEL*, A COSO-LINKED FRAMEWORK. Exhibit 2.3 is an example of a public domain control model that the IMA will be using for ERM skills training called CARD®*model* that is linked to the original COSO 1992 and COSO SPC frameworks and has been referenced in a number of Institute of Internal Auditor and IMA publications. CARD® stands for Collaborative Assurance and Risk Design. It uses eight control categories versus the five primary control categories in COSO. This model puts higher importance on "Commitment," "Indicator/Measurement," and "Process Oversight" controls relative to the attention given in COSO 1992. Each of the eight control categories in this model relates to an element of an organization's control framework. Beneath each of the eight categories in Exhibit 2.4 there is a menu of the specific control elements that an organization could use to achieve the core control category objective. Supporting each subelement of control is a trigger question available from the IMA that helps people understand the purpose of the control. This framework has been developed and tested over the past 20 years and draws on COSO 1992 and the other national frameworks covered in this chapter, as well as the Malcolm Baldrige quality framework, as well as other control models including the Modern Comptrollership framework developed in the Canadian public sector. All control elements in COSO 1992 and COSO SPC frameworks are included in this COSO-linked framework, although they are organized under different control category headings.

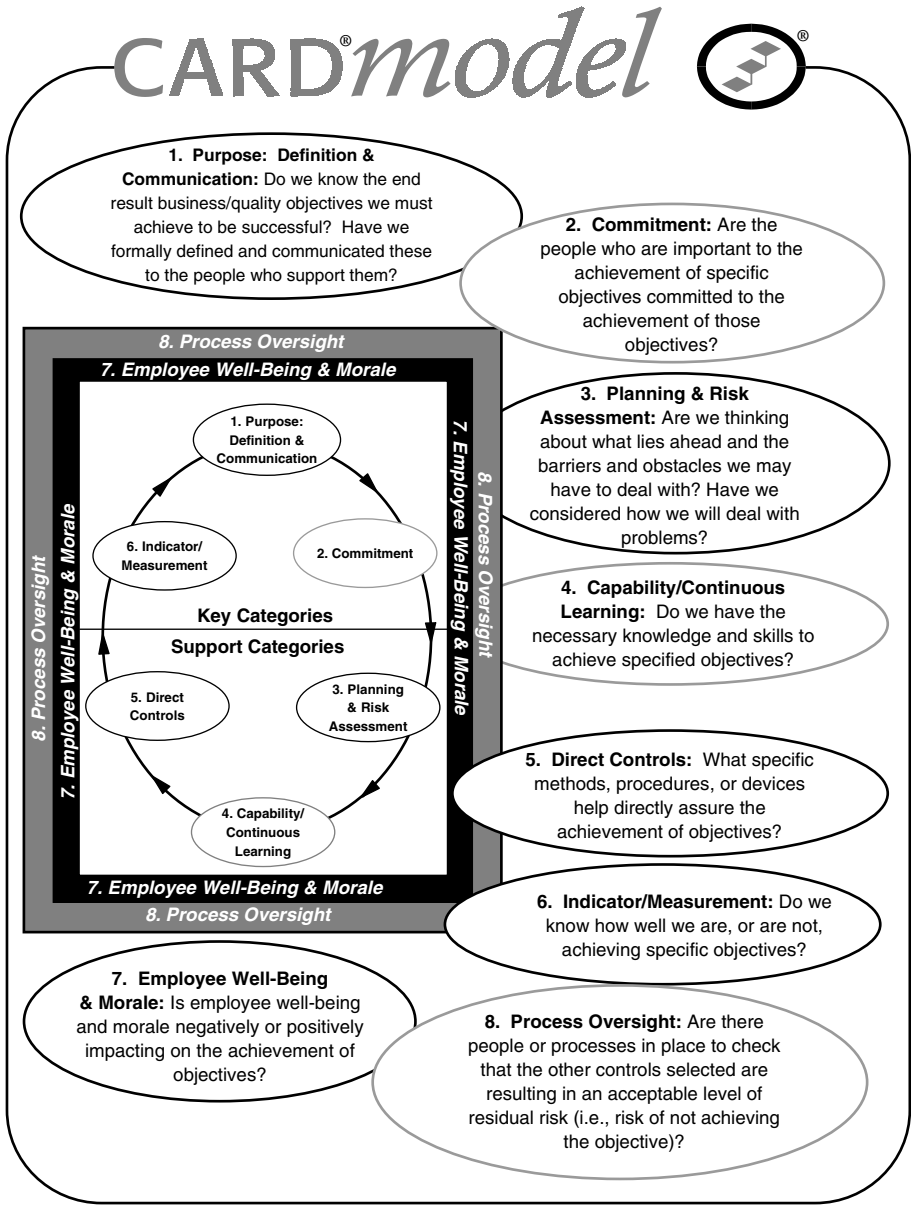
This reference aid can be used to identify existing or possible controls available to mitigate a particular risk and indicates to readers at a glance the mix of the type control design elements that are currently being used (e.g., a control design that lacks Indicator/Measurement controls or Commitment controls).

Here is an illustration of how this CARD®*model* methodology can be used for the same example used in the COSO 1992 section:

RISK

Senior management (Chief Executive Officer [CEO] and/or Chief Financial Officer [CFO]) overrides controls and improperly manipulates/falsifies financial statements.

Risk level rating assigned by management: high (i.e., extreme consequence with a moderate likelihood).



Source: © 2007 Institute of Management Accountants.

EXHIBIT 2.3 CARD®*MODEL*

1. PURPOSE: DEFINITION & COMMUNICATION

1.1 Definition of Corporate Mission & Vision
1.2 Definition of Entity-wide Objectives
1.3 Definition of Unit Level Objectives
1.4 Definition of Activity Level Objectives
1.5 Communication of Business/Quality Objectives
1.6 Definition and Communication of Corporate Conduct Values and Standards

2. COMMITMENT

2.1 Accountability/Responsibility Mechanisms
2.1a Job Descriptions
2.1b Performance Contracts/Evaluation Criteria
2.1c Budgeting/Forecasting Processing
2.1d Written Accountability Acknowledgments
2.1e Other Accountability/Responsibility Mechanisms
2.2 Motivation/Reward/Punishment Mechanisms
2.2a Performance Evaluation System
2.2b Promotion Practices
2.2c Firing and Discipline Practices
2.2d Reward Systems—Monetary
2.2e Reward Systems—Nonmonetary
2.3 Organization Design
2.4 Self-Assessment/Risk Acceptance Processes
2.5 Officer/Board Level Review
2.6 Other Commitment Controls

3. PLANNING & RISK ASSESSMENT

3.1 Strategic Business Analysis
3.2 Short-, Medium-, and Long-Range Planning
3.3 Risk Assessment Processes—Macro Level
3.4 Risk Assessment Processes—Micro Level
3.5 Control & Risk Self-Assessment
3.6 Continuous Improvement & Analysis Tools
3.7 Systems Development Methodologies
3.8 Disaster Recovery/Contingency Planning
3.9 Other Planning & Risk Assessment Processes

4. CAPABILITY/CONTINUOUS LEARNING

4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes
4.2 Self-Assessment Forums & Tools
4.3 Coaching/Training Activities & Processes
4.4 Hiring and Selection Procedures
4.5 Performance Evaluation
4.6 Career Planning Processes
4.7 Firing Practices
4.8 Reference Aids
4.9 Other Training/Education Methods

5. DIRECT CONTROLS

5.1 Direct Controls Related to Business Systems
5.2 Physical Safeguarding Mechanisms
5.3 Reconciliations/Comparisons/Edits
5.4 Validity/Existence Tests
5.5 Restricted Access
5.6 Form/Equipment Design
5.7 Segregation of Duties
5.8 Code of Accounts Structure
5.9 Other Direct Control Methods, Procedures, or Things

EXHIBIT 2.4 CARD®*MENU* DETAILED LISTING OF ELEMENTS

6.	**INDICATOR/MEASUREMENT**
6.1	Results & Status Reports/Reviews
6.2	Analysis: Statistical/Financial/Competitive
6.3	Self-Assessments/Direct Report Audits
6.4	Benchmarking Tools/Processes
6.5	Customer Survey Tools/Processes
6.6	Automated Monitoring/Reporting Mechanisms & Reports
6.7	Integrity Concerns Reporting Mechanisms
6.8	Employee/Supervisor Observation
6.9	Other Indicator/Measurement Controls
7.	**EMPLOYEE WELL-BEING & MORALE**
7.1	Employee Surveys
7.2	Employee Focus Groups
7.3	Employee Question/Answer Vehicles
7.4	Management Communication Processes
7.5	Personal and Career Planning
7.6	Diversity Training/Recognition
7.7	Equity Analysis Processes
7.8	Measurement Tools/Processes
7.9	Other Well-Being/Morale Processes
8.	**PROCESS OVERSIGHT**
8.1	Manager/Officer Monitoring/Supervision
8.2	Internal Audits
8.3	External Audits
8.4	Specialist Reviews & Audits
8.5	ISO Review/Regulator Inspections
8.6	Audit Committee/Board Oversight
8.7	Self-Assessment Quality Assurance Reviews
8.8	Authority Grids/Structures & Procedures
8.9	Other Process Oversight Activities

Source: © 2007 Institute of Management Accountants.

EXHIBIT 2.4 (*continued*) CARD®*MENU* DETAILED LISTING OF ELEMENTS

MITIGATING CONTROLS

CEO/CFO hiring practices—Element 4.4: Capability/Continuous Learning: Hiring and Selection Procedures

Audit committee oversight—Element 8.6: Process Oversight: Audit Committee/Board Oversight

Confidential concerns reporting line—Element 6.7: Indicator/Measurement: Integrity Concerns Reporting Mechanisms

Internal audit reviews—Element 8.2: Process Oversight: Internal Audits

External auditor audit of financial statements—Element 8.3: Process Oversight: External Audits; Element 6.1: Indicator/Measurement: Results and Status Reports/Reviews

The CARD®*model* framework was specifically designed to assist people with the task of identifying the controls currently in use that mitigate specific risks identified to a given macro- or micro-level assurance context and help them to understand what controls they could use if current performance or error rate for any assurance context is unsatisfactory.

(c) TREAT RISKS USING COBIT/ISO 17799/ITIL. Common risks that emerge when identifying and evaluating risks to the overall reliability of the financial statements and the line items and notes that comprise them relate to five broad areas:

1. Software programs do not correctly calculate/allocate/handle transactions that impact on the financial statements.
2. Accidental or intentional unauthorized/inappropriate modifications are made to software programs.
3. There is unauthorized/inappropriate/fraudulent modification of data in the system that is used to calculate/process accounting entries.
4. Unauthorized/inappropriate/fraudulent creation and submission of data is made to the accounting system.
5. Spreadsheets used to feed or produce accounting entries or notes are inaccurate/unreliable/not secure.

The controls that mitigate these types of risks are most generally called IT general controls.

For U.S. listed companies, PCAOB Audit Standard Number 2 (AS2) mandates that external auditors must independently assess IT general controls that impact the financial statements when completing SOX 404(b) assessments. In the absence of any guidance from the SEC on the subject, management has, by extension, used the general IT controls assessment requirements outlined in PCAOB AS2 related to IT general controls. The IT general controls area of external auditor evaluation has attracted a high number of complaints having a common theme that registrants believe that their external auditors and/or consultants have required an excessive amount of work on this dimension of control, resulting in high ongoing costs.

A precedent-setting paper calling for convergence and integration of competing IT standard-setting bodies titled "Aligning COBIT, ITIL, and ISO 17799 for Business Benefits: A Management Briefing from ITGI and OGC" suggests that:

> Every organization needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. All three can play a very useful part—COBIT and ISO 17799 helping to define *what* should be done and ITIL providing the *how* for service management aspects.[1]

(d) TREAT RISKS USING THE OCEG FOUNDATION FRAMEWORK. For risks that relate directly to business ethics and the ethics of individual senior executives, a framework that has been developed by the Open Compliance and Ethics Group (OCEG) is particularly relevant. It provides considerable detail on tangible methods companies can use to mitigate specific ethics and legal compliance risks. Considerable work and input have gone into the development of this framework, and it has undergone a very rigorous exposure and comment process. This framework is particularly relevant to the types of risks that caused SOX to be enacted in the United States.

2.7 IDENTIFY, ASSESS, AND REPORT ON RESIDUAL RISK STATUS

Once the assurance contexts to be assessed have been decided on; relevant risks have been identified, prioritized, and evaluated; and the mitigating controls for those risks have been identified and documented, the last step is determining the current residual risk status. This sequence can also be reversed wherein a company monitors the residual risk status for a given assurance context and completes a formal risk and control assessment to determine the cause only when the residual risk status information indicates a problem. The option of monitoring key performance indicators and key risk indicators prior to completing full assessments is not available to U.S. listed companies that must comply with the current SOX regulations for Sections 302 and 404.

Residual risk is defined in the AS/NZ 4360 Risk Management standard as "the risk remaining after implementation of risk treatment." For ICFR, this is the risk that remains that financial statement line items and/or notes are or could potentially be materially wrong in whole or in part.

Residual risk status is a collection of information that helps management and audit committees decide whether the residual risk related to the goal of reliable financial disclosures is acceptable.

(a) TYPES OF RESIDUAL RISK STATUS INFORMATION. Concerns. Concerns (also known as issues or review findings) are real or potential situations that have been identified where the current controls in place do not, or might not, mitigate one or more risks in whole or in part. Management must then decide whether the situation represents an acceptable concern or an unacceptable concern. In many companies, concerns explicitly or implicitly deemed acceptable are often not documented. An example is an accounting balance that involves estimates requiring a high level of judgment and experience. A risk is that inexperienced staff making the estimates make serious mistakes. The current employee who is making the judgments is new to the industry and the position and lacks knowledge and experience. This creates a residual risk concern. In the absence of adding other compensating controls, this produces a residual risk concern that is either acceptable or unacceptable to senior management. We encourage companies to document residual risk concerns that they elect to accept at a point in time, because new information may emerge and a concern that was acceptable at a point in time may not be down the road because of differences in circumstances and/or risk tolerance.

It is very important that external auditors are made aware of situations where the controls may not mitigate one or more risks that threaten the reliability of one or more accounts or notes. In some percentage of these situations they can elect to increase the substantive testing work they do to confirm the reliability of the accounts in question with the end result that the goal of reliable auditor-certified financial statements is still achieved. In other situations, it may not be possible or it may be very expensive to reduce the risk of financial statement

error. An example of this type of situation is when accounting program change controls or data access controls are unreliable and the impacted account balances are not amenable to reliable external auditor confirmation (e.g., whether a program functioned consistently and correctly throughout an entire accounting period without unauthorized changes). Auditors are placed in a very difficult situation when IT general controls are seriously deficient, because audit theory dictates that extensive work must be done to achieve a high level of audit assurance.

Indicator Data. This is information about how well a given assurance context is being met. (*Note:* This is not whether controls were performed as described but rather the degree to which the controls are actually mitigating risks to the assurance context being assessed.) An ICFR example is a company discloses in its 10-K that it has a profit before tax of $100 million. The auditor has given a clean opinion on the financial statements and an opinion that ICFR is effective in accordance with COSO. It is subsequently determined that $30 million of inventory shown on the balance sheet does not exist and the financial statements for the period must be restated. The assurance context is that inventory balances are reliable. The new information that has surfaced helps illustrate how well the controls worked to mitigate one or more risks. For an individual account balance, indicator data could be a material error discovered by the external auditor after management has signed off on the financial statements, or information that emerges in a subsequent accounting period and management is now aware that statements filed with the SEC contained some level of material error. Other less obvious examples might be an abnormal number of credit notes that must be issued in the first quarter of the year because the customers deny that they actually ordered the goods that were included in the prior period's sales. This is indicator data that the assurance contexts of reliable accounts receivable and sales were not met in part for that year-end.

Impact Data. This is information that helps decision makers understand the consequences that will or could flow from specific errors in the company's financial statements. Errors that impact only on classifications within similar balance sheet or income statement classifications are generally not as serious as balance sheet errors that impact on the income reported. Errors in some balance sheet accounts or notes to the financial statements, however, could have an impact on debt covenants, triggering a loan repayment, credit rating review, or other major consequences. An example would be errors in a note disclosure that is used extensively by security analysts that track a particular industry. The likely impact of financial statement errors is an area that is complex with few hard-and-fast rules. Investors sometimes appear to have fairly high tolerance to certain types of accounting errors but react drastically to others. A related area that is currently being debated on a global level is what type and/or size of error should result in a restatement of prior-period financial statements.

Impediment Data. In some situations there may be risks that threaten the reliability of accounting disclosures that are very difficult, expensive, or even

impossible to mitigate to a tolerable level because of one or more circumstances. An example might be a company that is developing new products or services that have not existed previously anywhere in the world. The absence of historical/corporate memory or awareness of these risks can cause material accounting errors. Another example of an impediment would be a legal decision handed down or an out-of-court settlement reached late in an accounting period in a case a company in the same industry is involved in that has the potential of materially impacting a company's valuation of one or more accounts. It may not be possible or practical to access this information on a timely basis. A very simple example may be a situation where a majority shareholder has dictated that an unqualified individual who lacks the necessary knowledge or skills fill a key accounting position like CFO or controller. The only viable mitigation for the type of risks that would flow from this situation is the skill of the external auditor in finding and correcting errors and/or highly competent personnel in the controllership department.

Transfer/Risk-Sharing Information. This is information about situations where some or all of the responsibility to mitigate risks has been shared or contractually transferred to another party. For ICFR, an example is outsourcing all responsibility for the company's pension fund management, including the design and operation of controls, to ensure accounting balances are reliable. Under current U.S. rules, this may require that the organization that is doing the accounting have an SAS 70 review of its controls. Determining that one has been done may (or may not) be enough to discharge a company's responsibility to ensure its own financial statements are reliable.

2.8 CONCLUDING REMARKS

This guide outlines a risk-based approach to ICFR that meets globally accepted risk management standards. The SEC and PCAOB will be issuing new revised guidance to SEC registrants on how to assess and report on ICFR. It is not clear at the time of writing that the new SEC/PCAOB regulatory expectations will allow registrants to use the type of globally accepted risk-based approach described in this chapter. Interested readers should visit the Institute of Management Accountants web site (www.imanet.org), for the IMA's comments on the 2007 guidance issued by the SEC and PCAOB. The IMA comment paper will specifically address whether the new, revised SEC/PCAOB ICFR guidance allows registrants to use globally accepted risk management principles in this area. Other IMA educational resources include two Statements on Management Accounting (SMAs) on the subject of Enterprise Risk Management (ERM), available to members and nonmembers for free.

Notes

1. ITGI and OGC, "Aligning CobiT®, ITIL®, and ISO 17799 for Business Benefit: A Management Briefing from ITGI and OGC, November, 2005.

CHAPTER 3

COSO—IS IT FIT FOR PURPOSE?

Tim Leech

The title of this chapter begs a question: What is "it"? Many think the term COSO refers to a now fairly dated four-volume control framework originally issued in 1992, titled Internal Control—Integrated Framework. Others know that COSO is the commonly used name for an unincorporated, loosely constituted private sector committee formed in the United States in 1985 in response to the savings and loan crisis. This chapter explores two important questions:

1. Is COSO, the committee originally formed over 20 years ago to sponsor a research study, commonly known as the Treadway Commission after its chairman, James C. Treadway, as currently constituted still fit for purpose?
2. More important, is the 1992 Internal Control—Integrated Framework, a COSO Committee work product now approaching its 15th birthday, up to the task of meeting new, complex, onerous, and hugely important expectations imposed on it by the Securities and Exchange Commission (SEC) to serve as generally accepted risk and control assessment principles (GARCAP) for major public and private sector organizations around the world?

For those who like to cut to the chase, the answer proposed here is an unequivocal *no* to both questions.

3.1 THE ROOTS OF COSO

In the 1970s, as a result of a series of highly publicized corporate reporting failures and a loud public outcry, the American Institute of Certified Public Accountants funded the Commission on Auditor's Responsibilities, better known as the Cohen Commission. The Commission's task was to:

> develop conclusions and recommendations regarding the appropriate responsibilities of independent auditors. It should consider whether a gap may exist between what the public expects and needs and what auditors can and should reasonably expect to accomplish. If such a gap does exist, it needs to be explored to determine how the disparity can be resolved.

A key element of the study was to determine why an alarming number of external auditor opinions on public company financial statements were subsequently being proven wrong. To reduce the incidence of auditor opinion failure, the Commission concluded that:

> A major step in implementing the Commission's proposed evolution, which should be adopted as soon as possible, would require the auditor to expand his study and evaluation of the controls over the accounting system to form a conclusion on the functioning of the internal accounting control system. If the auditor finds material weaknesses in the internal accounting control system, and those weaknesses are not corrected, material deficiencies may occur in the preparation of accounting information or in the control of the corporation's assets.

This visionary 1977 recommendation was, unfortunately and for all intents and purposes, ignored. The chairman of the landmark Cohen Commission, Manuel F. Cohen, died before the Commission's report was released.

In 1985 five not-for-profit organizations—the American Institute of Certified Public Accountants, the American Accounting Association, the Institute of Internal Auditors, the National Association of Accountants (now the Institute of Management Accountants), and the Financial Executives Institute—banded together and formed the Committee of Sponsoring Organizations of the Treadway Commission to sponsor and fund another study of what had, once again, become a highly visible and widespread problem: fraudulent financial reporting. The chairman of the Commission was James C. Treadway, Jr. That committee became best known as a result of self-proclamation as COSO. COSO's stated founding mission in 1985 was "to identify causal factors that can lead to fraudulent financial reporting and steps to reduce its incidence"—an ambitious and noble goal at the time that is still relevant today.

In October 1987 the Treadway Commission's final report recommended: "The Commission's sponsoring organizations should cooperate in developing additional, integrated guidance on internal control."

Another key recommendation of the Treadway Commission built on recommendations made by the Cohen Commission a decade earlier:

> All public companies should be required by SEC rule to include in their annual reports to stockholders management reports signed by the chief executive officer and the chief accounting officer and/or the chief financial officer. The management report should acknowledge management's responsibilities for the financial statements and internal control, discuss how these responsibilities were fulfilled, and provide management's assessment of the effectiveness of the company's internal controls.

This visionary recommendation that a public company's management should formally acknowledge responsibility for, and report on, the effectiveness of internal control was, for all intents and purposes, ignored for another 15 years until the signing of the Sarbanes-Oxley Act in 2002.

As a direct result of the Treadway Commission recommendation in 1987 that the Commission's sponsoring organizations develop guidance on internal control, the Committee of Sponsoring Organizations of the Treadway Commission, now known generally as the COSO Committee, developed and issued a groundbreaking exposure draft on March 12, 1991, titled Internal Control—Integrated Framework. The primary authors of this framework were partners and staff of Coopers & Lybrand, one of the big eight auditing firms in existence at the time. (*Note:* Coopers & Lybrand has now become PricewaterhouseCoopers in the era of the big four.) The 1991 COSO framework exposure draft illustration defining the term *internal control* is shown in Exhibit 3.1.

(a) THE DEFINITION. Internal control is the process by which an entity's board of directors, management, and/or other personnel obtain reasonable assurance as to achievement of specified objectives; it consists of nine interrelated components, with integrity, ethical values, and competence, along with the control environment, serving as the foundation for the other components, which are: establishing objectives, risk assessment, information systems, control procedures, communication, managing change, and monitoring.

As a result of an aggressive counterlobby from the old-guard auditor faction, the final version of Internal Control—Integrated Framework released in 1992 reduced the number of control categories from nine categories to five and made major changes to the definition of internal control to make it more closely conform to definitions that had been in use in the United States by external auditors for many years:

> a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations

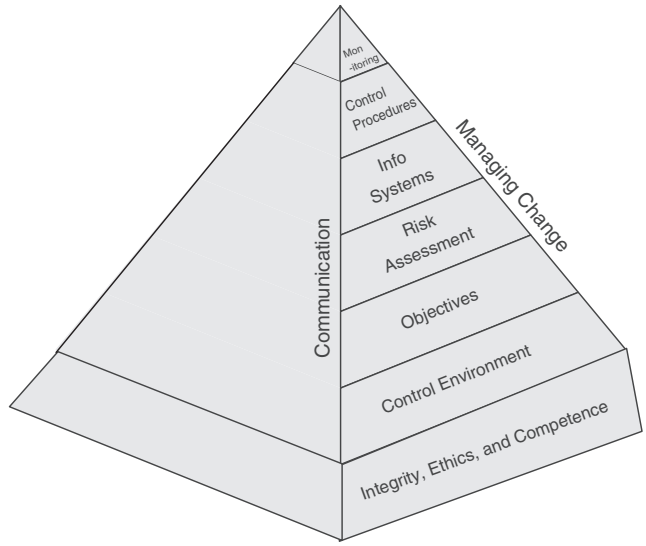


EXHIBIT 3.1 COSO 1991 EXPOSURE DRAFT PROPOSAL

This framework identified five interrelated components—control environment, risk assessment, control activities, information and communication, and monitoring. A diagram depicting the COSO 1992 framework is shown in Exhibit 3.2.

By far the most hotly debated change between the COSO 1991 exposure draft and the 1992 final framework was the treatment of the "objectives" component. The 1992 version of the framework indicates that the decision was that the establishment of entity-level objectives, including mission and value statements and strategic planning, is a "management activity" but not part of an integrated control framework (page 17 of the 1992 framework volume). This was explained at the time:

> The "objectives" component has been eliminated as a separate component. The view expressed by some respondents that the establishment of objectives is part of the management process, but it is not part of internal control, was adopted. The final report recognizes this distinction, and discusses objective setting as a precondition to internal control.[1]

The decision to eliminate the objectives category as an element of internal control in 1992 has now been, at least in part, contradicted by the COSO Committee's July 2006 Smaller Public Company (SPC) guidance. That report states:

> The COSO framework recognizes that an entity must first have in place an appropriate set of financial reporting objectives. At a high level, the objective of financial reporting is to prepare reliable financial statements, which involves attaining reasonable assurance that the financial statements are free from material misstatement. Flowing from this high-level objective, management

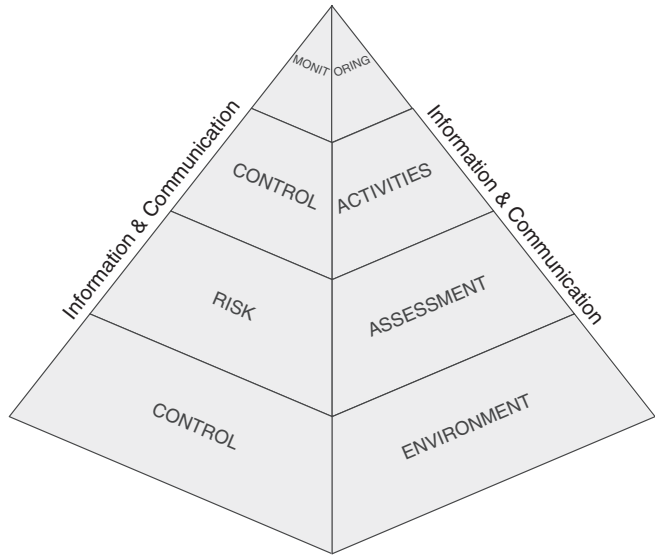


EXHIBIT 3.2 COSO 1992 FINAL FRAMEWORK

establishes supporting objectives related to the company's business activities and circumstances and their proper reflection in the company's financial statement accounts and related disclosures. These objectives may be influenced by regulatory requirements or by other factors that management may choose to incorporate when setting its objectives.[2]

Apparently readers are asked to accept that the establishment of objectives is central to effective control but not part of an integrated internal control framework. This logic has been rejected by teams in the United Kingdom and Canada who studied the strengths and weaknesses of the 1992 framework prior to making their own proposals for the elements of an integrated control framework.

3.2 COSO THE COMMITTEE AND COSO THE 1992 INTEGRATED CONTROL FRAMEWORK: HAVE THEY STOOD THE TEST OF TIME?

It is important to note that the 1992 version of the COSO Internal Control—Integrated Framework has not been modified in any significant way since it was released more than 14 years ago. Unlike the Malcolm Baldrige and ISO quality frameworks, which both require that the criteria be regularly revisited and improved based on user feedback, there is no similar improvement process in place for the COSO 1992 framework. Some of the COSO Committee member organizations have claimed that this is because the 1992 framework has stood the test of time. The Institute of Management Accountants, a founding member of COSO, has voiced concerns on this point but to date has been unable to get

the support of the other COSO Committee members to undertake an update of the framework.

The fact that there is no improvement process in place for the 1992 COSO Internal Control—Integrated Framework is likely explained by the fact that COSO is, in reality, not an organization in the usual sense but rather a loosely constituted committee that meets a few times a year. As a committee it has no legal existence, no corporate governance structure, no funding mechanisms, and no physical address, and it is not overseen by any regulatory body. There is also currently no mechanism in place to fund the COSO Committee's projects beyond contributions from sponsoring organizations. To illustrate its financial limitations, the COSO Committee has recently released a request for proposal (RFP) for a consulting firm to help with its latest project on monitoring of internal control. Firms interested in bidding are cautioned in the COSO RFP issued on October 17, 2006, that:

> COSO is a volunteer committee with limited resources. Typically the COSO Board has reimbursed developers for out-of-pocket expenses only (e.g., reasonable travel and administrative costs). The business benefit to the developer is that the developer is identified directly with the COSO end-product as part of the globally recognized COSO brand.

What this caution really means is that those that apply to act as primary COSO researchers and authors should be prepared to accept public relations benefits in lieu of being paid. This pro bono/donation approach to research and standard writing has been how the majority of work undertaken by the COSO Committee to date has been done, including the guidance issued by the COSO Committee on enterprise risk management (ERM) in 2004 and guidance for smaller public companies (SPC) issued in 2006. Both of these more current work products are heavily linked to the original, unchanged 1992 five-category framework. Both of these work products were authored by PricewaterhouseCoopers in return for the right to be formally linked to the COSO brand.

It is important to note that since the COSO Internal Control—Integrated Framework was released in 1992, the committee has made no attempt to rigorously monitor acceptance and use of the framework or periodically assess in a formal way whether the framework could, and should, be improved. The rigorous analysis of the strengths and weaknesses of the COSO 1992 framework that has been done in other countries in the mid-1990s, including Canada and the UK, has not been formally acknowledged by the COSO Committee.

3.3 ACTUAL MARKET ACCEPTANCE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX

Voluntary market acceptance of the value of the COSO 1992 framework as a tool for management and auditors prior to the enactment of Sarbanes-Oxley can be seen from the statistics in Exhibit 3.3. These findings are part of a rigorous

	Q1: Extent to which COSO 1992 is utilized by our company to manage its enterprise risk and controls		
Response Scale	Overall Sample (N = 373) % of Total	Internal Auditors (N = 146) % of Total	Management Types (N = 227) % of Total
1. No Extent	37.8% (141)	45.9% (67)	32.6% (74)
2. Some Extent	31.4% (117)	30.1% (44)	32.2% (73)
3. Moderate Extent	13.9% (52)	11.6% (17)	15.4% (35)
4. Large Extent	11.3% (42)	7.5% (11)	13.7% (31)
5. Not Sure	5.6% (21)	4.8% (7)	6.2% (14)

Exhibit 3.3 Use of the COSO 1992 Framework Prior to SOX by Company Management

research study on the use of the COSO 1992 framework conducted by Professor Parveen Gupta under the sponsorship of the Institute of Management Accountants.

The largest number of respondents indicates that the 1992 COSO framework was not used to any extent in their company prior to the enactment of the Sarbanes-Oxley Act in 2002. Only a very small number of companies indicate that they used the COSO 1992 framework to a large extent.

During the period of 1992 to 2002 the Institute of Internal Auditors and the American Institute of Public Accountants, two of the five founding members of the COSO Committee, made some attempts to promote and educate their members on the value and benefits of using the COSO control framework through training workshops, publications, and integration with certification curriculum, although limited knowledge of COSO 1992 was required for certification in these organizations. The other three COSO founding members did relatively little during this period to aggressively promote why, or how, the COSO 1992 Internal Control—Integrated Framework could or should be used by their members. The business case for using the COSO framework has not been well articulated, communicated, or accepted by the majority of the business community.

3.4 EXPECTATIONS OF COSO ESCALATE OVERNIGHT

When the SEC released final guidance for Section 404 in 2003, as a general statement, it mandated the use of the COSO control framework for assessing internal control over financial reporting by every public company listed on a U.S. exchange by stating that the COSO 1992 Internal Control—Integrated Framework

met the SEC's four suitability criteria for SOX control assessments. The SEC said that to qualify as a suitable assessment framework the framework must:

1. Be free from bias.
2. Permit reasonably consistent qualitative and quantitative measurements of a company's internal control.
3. Be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted.
4. Be relevant to an evaluation of internal control over financial reporting.

Although the SEC said in footnote 67 of Section 404 final rule, "The Guidance on Assessing Control issued by the Canadian Institute of Chartered Accountants and the Turnbull Report published by the Institute of Chartered Accountants in England & Wales are examples of other suitable frameworks," it was unequivocal when it stated:

> The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements.

Concluding that the 1992 COSO Internal Control—Integrated Framework was capable of fully meeting all four criteria was a massive untested assumption on the part of the SEC that has now been identified as a major contributing factor to the massive confusion and costs that have occurred as U.S. listed public companies attempted to comply with sections 302 and 404 of SOX.

3.5 IS COSO 1992 FREE FROM BIAS?

In real life the goal of producing work products that are totally free of any bias is an elusive one. When we are asked as individuals to undertake any task in life, it is very difficult if not impossible not to bring our collective experiences and biases to the table. All COSO work products to date have been produced by professionals who have an audit bias. Although the COSO Committee members include organizations that represent management accountants, financial executives, internal auditors, accounting academia, and external auditors, the perspectives and historical viewpoints of the internal and external audit professions have dominated to date. Many internal auditors have external audit backgrounds. An external auditor background generally results in viewpoints that are quite different from those held by others engaged in assurance activities like quality professionals, risk professionals, IT specialists, or even generic management consultants. The biases are influenced by the training and accreditation process for their respective disciplines.

The term *internal control* is itself an internal/external auditor invention that doesn't exist in any real way in the realm of quality or risk management, and is rarely used by business unit staff in their daily work. Quality professionals

use frameworks like Malcolm Baldrige, six sigma, ISO 9000, and ISO 17799 as their frameworks to ensure that desired outcomes are achieved. They talk about ensuring process reliability. Risk professionals use philosophies found in frameworks like the Australia/New Zealand Risk Management standard 4360. They talk about achieving the goal of assessing and analyzing risk and seeking agreement on acceptable levels of residual risk. IT professionals use frameworks like Control Objectives for Information Technology (CobiT) and Information Technology Infrastructure Library (ITIL). Their goal is usually to examine a client's environment for conformance to those frameworks. Management consultants use methodologies like balanced scorecards and talk in terms of strategic priorities, key result areas, and key performance indicators.

Is COSO 1992 free from bias? From a purist perspective, COSO Committee work products produced to date have *not* been free from bias.

3.6 DOES COSO 1992 PERMIT CONSISTENT QUANTITATIVE/QUALITATIVE MEASUREMENT?

Evaluation frameworks such as Malcolm Baldrige put enormous emphasis on the importance of measurement controls in the pursuit of quality. Baldrige, unlike the COSO Internal Control—Integrated Framework, is a numerically weighted framework that allows a score to be generated on a company's quality system out of total possible 1,000 points. None of the COSO frameworks have numeric weightings or any type of guide for management or auditors to assign numeric scores. Very little guidance is provided for users on how to evaluate qualitative information and reach "effective/ineffective" conclusions on internal control, although the 2006 COSO guidance for smaller public companies (SPC) did make advances in this area. To meet this suitability test, a framework would have to be capable of generating reasonably consistent conclusions from multiple teams when given the same set of facts. None of the three primary COSO guidance documents produced to date (COSO Internal Control—Integrated Framework, COSO ERM, or COSO SPC) were ever intended or designed to accomplish this goal.

From just about any perspective, the COSO Committee work products produced to date do not permit reasonably consistent quantitative/qualitative measurements of internal control.

3.7 IS COSO 1992 SUFFICIENTLY COMPLETE SO THAT RELEVANT FACTORS ARE NOT OMITTED?

The original mission of the Treadway Commission was "to identify causal factors that can lead to fraudulent financial reporting and steps to reduce its incidence." A key recommendation was to develop an internal control framework that would support this aim. The current SOX requirements issued by the Public Company Accounting Oversight Board (PCAOB) call for a specific analysis of the control capabilities to prevent and detect fraud. An Institute of Management Accountants (IMA) research study completed in September 2006 on the use of COSO 1992

for SOX indicated that very few companies used the COSO 1992 framework as the primary assessment guidance to do this task. On average, less than one in four respondents indicated that they used COSO 1992 to a large extent to complete this dimension of their assessments. Other surveys conducted indicate that most companies used guidance issued by the Association of Certified Fraud Examiners or the AICPA to examine the existence and quality of controls. The IMA study also indicated that more than 25 percent of respondents indicated that they did not complete any formal antifraud assessment.

On other fronts, most people acknowledge that in today's world, IT plays a huge role in the processes used to generate external financial disclosures and that weak IT controls can result in material errors in financial statements. The same IMA research study indicated that more than 60 percent of respondents did not use COSO 1992 to assess the adequacy of IT controls. Almost 52 percent of respondents indicated they used the CobiT framework issued by the IT Governance Institute.

Unless one accepts that fraud prevention and detection and IT are not relevant factors when opining on the adequacy of internal control over financial reporting, the COSO framework does not meet the criterion of being complete.

3.8 IS COSO 1992 RELEVANT TO AN ANALYSIS OF CONTROLS OVER FINANCIAL REPORTING?

The events that resulted in the enactment of SOX had a common theme—a significant breakdown of oversight and ethics at senior levels of public companies, including the audit committees of these corporations. Most people with knowledge of the facts that led to SOX agree that the number one risk to reliable financial reporting is a lack of ethics on the part of senior-level employees. Although there are no hard statistics available, there is evidence that supports the view that the second biggest risk to reliable financial disclosures is inadequate knowledge/capability on the part of senior financial accounting staff. The unverified third biggest risk, although one could advance an argument that it is the number one risk, is the competence and integrity of the external auditors hired to audit and report on the financial statements produced by management.

While it is indisputable that COSO 1992 does include some discussion of the need for an ethical tone at the top, it provides little in the way of specifics on how to measure whether controls to ensure sound ethics are effective. If one wants to see a framework that emphasizes how to evaluate the adequacy of controls important to compliance and ethics, the best and newest guidance available is from a new organization called Open Compliance and Ethics Group (OCEG) (www.oceg.org). COSO 1992 certainly does not provide much, if any, specific guidance on how to evaluate the controls to ensure that financial accounting personnel possess sufficient competence or the controls at CPA firms to ensure high ethical conduct on the part of partners and staff. Again, the newer COSO SPC framework has made some advances in this area.

COSO is relevant but not optimal for evaluating the adequacy of controls to address the three biggest risks to reliable financial reporting.

3.9 COSO: LOOKING FORWARD

Concerns regarding the adequacy of the COSO Internal Control—Integrated Framework have been reported by a wide range of respondents to the SEC and PCAOB. The SEC has not directly addressed the question of the challenges that have been raised regarding the suitability of COSO 1992, or the brand-new COSO for Smaller Public Companies guidance, but indirectly has signaled an answer. The SEC has announced plans to develop and issue its own guidance on how to assess and report on internal control. This guidance is expected to be issued in an exposure draft form. The IMA has publicly stated that they believe that the COSO 1992 was never intended to meet the criteria defined by the SEC and that it does not fully meet all of the defined suitability criteria for SOX. To date none of the other COSO Committee organizations have publicly stated their position as to whether the 1992 COSO Internal Control—Integrated Framework fully meets all four of the suitability criteria defined by the SEC.

In a letter to the SEC dated September 18, 2006, in response to an SEC request for comments on a concept release related to SOX (www.sec.gov/comments/s7-11-06/s71106-98.pdf), Larry Rittenberg, the current chair of the COSO Committee, closed with the following hints on the way forward:

> COSO is embarking on a strategic planning process to adapt to the changing environment. The COSO Board has recognized that a new infrastructure may be needed for COSO to address internal control and risk management issues on a more timely fashion. The Board has discussed projects such as using the Internet to enhance the sharing of control information, a project on assessment, and a project identifying effective monitoring of controls. The Board also seeks to address many longer-term issues, such as harmonizing control frameworks and becoming more inclusive as an organization. The Board is committed to improving the practice of internal control implementation as well as internal control reporting on a more cost-effective manner for all firms. We welcome the opportunity to work with the SEC in accomplishing our mutual objectives in this area. We seek the SEC's input on these important endeavors.

Time will tell whether COSO the framework or COSO the committee are fit for purpose. Stay tuned.

Notes

1. Internal Control—Integrated Framework, 110. Framework Volume: September 1992.
2. Volume II: Guidance, 10.

CHAPTER 4

TIME TO RETHINK THE CORPORATE TAX

Ann Cullen

4.1 Q&A WITH MIHIR DESAI

Published: Ann Cullen Interview in the Harvard Business School: Working Knowledge, "Time to Rethink the Corporate Tax System," July 18, 2005, (http://hbswk.hbs.edu/item/4902.html).

Corporations have traditionally considered taxes a painful but necessary cost of doing business. But this view has changed, says Harvard Business School professor Mihir A. Desai. With the advent of sophisticated tax shelters, global tax-reduction opportunities, and high-priced finance experts focused on the issue, corporations are turning the tax function into a profit center, says Desai, an expert on international corporate and public finance.

In this e-mail interview, Desai discusses new ways businesses are looking to shrink their tax obligations, how the commonly accepted dual-book system may ultimately harm shareholders, and the role boards of directors play in making sure their companies stay within the rules.

Ann Cullen: How has the way corporations view taxation changed?

Mihir A. Desai: There is growing evidence that the tax function within corporations has shifted from being a compliance function to being a profit center. The ratio of corporate taxes to gross domestic product (GDP) declined through the late 1990s even during an economic expansion. There has been a growing disconnect between the income reports to capital markets and to tax authorities (a by-product of the dual-book system where firms characterize profits to tax authorities and capital markets separately).

There is also much anecdotal evidence on the profusion of tax shelters and compensation incentives for managing effective tax rates. Managers appear to have become more attuned to the possibilities of creating profits by minimizing tax obligations.

Q: You mentioned the dual-book system. Why are firms allowed to report their profits in two different ways to capital markets and tax authorities?

A: It is a curious system. Imagine if you were allowed to report income to the IRS in one way and on your mortgage application in another way. You might, in a moment of weakness, depict your situation in a particularly favorable light to your prospective lender and make yourself look worse off to the IRS. Indeed, you might end up with two completely different pictures of your economic situation that would serve your best interests.

With the growing globalization of firms and the growth of these discretionary opportunities, the dual-book system is clouding the true picture of how firms are actually performing.

Of course, you do not have this opportunity, and for good reason. Your lender can rest assured that the 1040 it reviews in deciding whether you deserve a mortgage would not overstate your earnings, given your desire to minimize taxes. Similarly, tax authorities can rely on the use of tax forms for other purposes to limit the degree of income understatement, given your need for capital. In that sense, the uniformity with which you are forced to characterize your economic situation provides a natural limit on opportunistic behavior that serves the interests of prospective lenders and tax authorities. This uniformity may even benefit you if it makes both reports more credible and eliminates doubts about your income.

While individuals do not have this opportunity, corporations do. Historically, accounting treatments deviated to allow for differential accounting of expenses. In the process, policymakers get a policy tool without distorting the way in which income is reported to capital markets. For example, depreciation schedules for investment can be different for tax and accounting purposes, creating a tool for fiscal stimulus.

I think this rationale has outlived its usefulness for several reasons. For starters, these different definitions of such expenses no longer account for much of the difference between book and tax income, and yet this disparity has been growing. Other factors, such as the peculiar accounting treatment of stock option compensation and differential treatment of overseas income, subsidiary income, and pension obligations, account for some of this disparity, and a large portion remains unaccounted for but is consistent with tax sheltering. Moreover, investment lives have shortened considerably, removing much of the power of accelerated schedules.

With the growing globalization of firms and the growth of these discretionary opportunities, the dual-book system is clouding the true picture of how

firms are actually performing. As such, enforcing uniformity could reduce uncertainty over the level of true profits, thereby furthering the interests of unsure investors, tax authorities, and firms.

Q: What is driving this change in the way managers view corporate taxes?

A: I think several factors are at work. First, financial engineering increasingly allows for cheap recharacterizations of income for tax and book purposes, making tax obligations easily disappear.

Second, the growing global reach of companies and falling costs of global transactions mean that profits can be reallocated to lower-tax jurisdictions with a fair amount of ease.

Finally, changing patterns of incentive compensation have sharpened incentives to squeeze profits out of parts of the organization that were heretofore not profit centers.

Q: Is this necessarily a bad thing? This is good news for shareholders, is it not? In other words, lower corporate taxes just mean more profits for shareholders, correct?

A: You are absolutely right to think that this could be viewed as a good thing. Indeed, there are a variety of reasons to think of the corporate tax as distortionary, and reductions of that burden could be welcome. Moreover, if shareholders are the recipients of all this value, then this would just be a transfer from tax authorities to shareholders. Unfortunately, the evidence is more mixed on the degree to which shareholders benefit from these activities. Countering the tempting logic that tax avoidance is good for shareholders is the fact that tax avoidance opportunities require obfuscation and, consequently, open the door to managerial opportunism. Indeed, several high-profile cases of managerial opportunism, including Enron, Tyco, and Dynegy, had their genesis in tax-planning activities. These activities, and the secrecy they demanded, became the cover for activities that were not in shareholders' best interests.

Oversight of tax planning, much like accounting, can no longer be relegated to specialists within corporations.

There are other more systematic pieces of evidence that suggest that the link between reduced taxes and shareholder benefits is tenuous. Specifically, my coauthors and I have examined a crackdown in tax enforcement in Russia that was accompanied by an *increase* in share prices of those companies subject to the crackdown. In a setting where there is plenty of scope for managerial diversion, having the state enforce its claim can be a wonderful thing for shareholders. Similarly, tax avoidance in the United States is valued fully only for firms that are considered well-governed firms. Some apparently tax-motivated transactions such as corporate inversions are often not greeted with a positive price reaction.

In short, the view that tax avoidance is simply a net transfer of value from the state to shareholders is complicated by the agency problem between shareholders and managers.

Q: How should CEOs and boards of directors respond to this changing environment?

A: Because of increased activity by tax planners within corporations and the heightened attention to tax shelters by regulators, boards have to become attuned to what tax risks are being borne by shareholders.

Tax planning can be a legitimate, value-enhancing activity and, indeed, can be a competitive necessity. But tax planning can also cross the line into activity that is costly to shareholders. Creating the right incentives within organizations and ensuring transparency for these activities is critical. Oversight of tax planning, much like accounting, can no longer be relegated to specialists within corporations, given the risks that it entails.

Q: If both shareholders and tax authorities are potentially worse off from all this activity, what should be done about this more generally?

A: While firms are forced to do some minimal reconciliation of their tax reports and capital market reports, these reconciliations provide very limited detail (in tax forms) or are completely opaque to even the most nuanced analysts—take a look at the tax footnotes of any major corporation. As such, a minimal solution would be the clarification and elaboration of these differences in public documents.

More generally, a wholesale revisiting of the rationale for departing from conformity in the reporting of book and tax income seems long overdue. Given that financial report accounting has evolved over the years while tax accounting remains quite primitive, conformity on financial reporting definitions would seem to make sense. This change could prevent a variety of tax shelters, as managers seldom undertake tax shelters when they reduce book profits. This possibility does raise some concerns that capital market profit reporting will be driven by tax considerations. This concern has to be weighed against the gains in reduced compliance costs (firms would no longer have to file hundreds or thousands of returns) that are currently sizable, reductions in tax sheltering, and reduced opportunities for managerial manipulation created by book-tax differences. Simple calculations also indicate that book-tax conformity could reduce tax rates considerably, as a 15 percent tax on book-pretax profits (just for public companies) would provide the same amount of corporate tax revenues being collected today.

Most radically, these trends provide another reason to revisit the rationale for a corporate tax more generally. The corporate tax is hard to like, as it facilitates an additional layer of taxation on savings. If, in addition, the evasion of these taxes is widespread and this evasion is linked to managerial malfeasance, it is even harder to rationalize such a tax.

4.2 ABOUT FACULTY IN THIS ARTICLE

Mihir Desai is the MBA Class of 1961 Fellow and an associate professor at Harvard Business School.

(a) LINKS TO RELATED WORKS BY MIHIR A. DESAI. On the argument for book-tax conformity and the links between tax avoidance and accounting fraud in major corporate scandals, see "The Degradation of Reported Corporate Profits," forthcoming in the *Journal of Economic Perspectives*.

On the divergence between book and tax income, see (in PDF format) "The Divergence between Book and Tax Income," in James Poterba (ed.), *Tax Policy and the Economy* 17 (Cambridge, MA: MIT Press, 2003), 169–206.

On the nexus between tax avoidance and corporate governance internationally, see "Theft and Taxes," with I. J. Alexander Dyck and Luigi Zingales, NBER Working Paper 10978.

On the link between tax avoidance and high-powered incentives in the United States, see "Corporate Tax Avoidance and High Powered Incentives," with Dhammika Dharmapala, forthcoming in the *Journal of Financial Economics*.

On the way tax avoidance has been valued by financial markets in the United States, see "Corporate Tax Avoidance and Firm Value," with Dhammika Dharmapala, NBER Working Paper 11241.

On the determinants of multinational firm activity in tax havens, see "The Demand for Tax Haven Operations," with C. Fritz Foley and James R. Hines Jr., forthcoming in the *Journal of Public Economics*.

CHAPTER 5

THE ROLE OF INTERNAL AUDIT

Frank Edelblut
Hernan Murdock

5.1 INTRODUCTION

The role of internal auditors is to provide independent, objective assurance and consulting services to organizations in ways that improve their operations. The main objective is to help management achieve its business goals through a systematic and disciplined approach to evaluating and improving the effectiveness of management, control, and governance processes.[1] In this regard, the internal audit function can add value to the organization by identifying exposures and verifying that mitigating controls are designed appropriately and function as intended.

5.2 INTERNAL AUDITORS' ROLE THROUGHOUT HISTORY

Internal auditing as a practice and profession has a long and curious history. Some date the origin back 5,500 years ago when records of a Mesopotamian civilization showed tick marks to denote the verification of numbers. The history continues through the records of Egyptian, Persian, Hebrew, Greek, and Roman civilizations as well. Interestingly, and unfortunately, the Greeks are believed to have used slaves as auditors because they could torture them to reveal the truth.[2]

With the fall of Rome and the demise of monetary and control systems, the profession lost some of its prominence. It was not until the end of the Dark

Ages that the double-entry system of bookkeeping was born, and once again the need for accountability pressed independent verification to the forefront. This gained additional impetus as civilization expanded and overseas investments in new lands became the norm. Queen Isabella of Spain even sent an auditor with Christopher Columbus on his venture to discover the New World.[3]

In spite of these developments, however, the profession of internal auditing lived in the shadow of its more mature brother—the independent accountant and external audit—until 1941, when the Institute of Internal Auditors (IIA) was formed. At that time, the founders struggled to come up with a name that did not include "internal audit," believing that it too narrowly described the span of activities. Historical precedence triumphed, and the IIA has had a profound impact on the profession.[4]

While the IIA was developing its personality and purpose, activity proliferated in the area of organizational theory. Academic institutions, capitalizing on the lessons of the industrial era, developed theories that systematized the organization with centralization, a defined hierarchy, distinct authority levels, a firm discipline, clear rules, and the division of labor.[5]

Internal audit development kept pace with these theories. Companies were standardized in terms of how they functioned, so naturally internal auditors developed standardized approaches to audit those organizations. With consistent approaches came various checklists, standard audit programs, and common procedures. In essence, the practice of internal audit developed so that it validated the organization, its centralization, hierarchy, authority, discipline, rules, and division of labor against the standard model.[6] The audit function, operating at peak efficiency, was able to quickly assess control or operational effectiveness with this standardization.

Standardization carried a latent risk, however: It limited the need for creativity and creative thinkers in the profession. There was little impetus to change the standard approaches. Under the guise of (as well as the legitimate need for) independence, internal auditors isolated themselves from the businesses they supported, preferring to make recommendations and allow management to respond. This underlying risk became apparent starting around 1960 and lasted through the 1980s. While internal auditors were protecting their independence, the businesses they served were changing. Impacted by globalization and technological advancements, among other things, companies no longer operated using the standard model. With manufacturing in different countries, it was impractical to have a single procurement function with a lone manager of purchasing. With customers around the globe, approval of customer orders was no longer the function of the vice president of sales. Regional general managers in local countries were accepting customer orders and making revenue decisions. The controller no longer needed to manually approve credit memos. The Enterprise Resource Planning (ERP) system provided the necessary separation of duties and limited transaction processing to those authorized.

Many internal auditors missed the signs and were very slow to adapt to the business changes taking place. As a result, they became increasingly irrelevant. Still armed with the standard checklists and the standard business model, they continued to insist that outdated procedures be followed, such as having the vice president of sales approve all customer orders and the controller print out the credit memos and sign them.

Everyone accepted the need for effective internal auditing, and management agreed that a strong and reliable internal control environment was important. But management slowly lost confidence in an internal audit function that recommended changes to the business that were clearly out of step with how the company was functioning. Management questioned why some audits were even being performed.

It was this loss of confidence in many internal audit departments that created the opportunity for outside providers of internal audit services to prosper during the 1990s. Generally, management believed in the importance of having sound internal controls but did not believe that the in-house audit function was making an effective contribution to the company. While the major accounting firms rapidly entered into the market, others, too, saw the opportunity and took advantage of it, creating both captive (i.e., in-house) and merchant (i.e., outsourced providers) markets for internal audit.

As auditors slowly embraced the fact that the standard business model and the profession had changed, the dot-com explosive growth and meltdown in the late 1990s resulted in the enactment of the Sarbanes-Oxley Act of 2002 in the United States. Sarbanes-Oxley created a seismic shift in the profession and placed internal auditors in a critical role, helping publicly traded companies meet their compliance obligations under this new legislation. Year 1 was difficult; year 2 was a little easier, and by year 3 many companies were moving quickly toward the institutionalization of this compliance effort. What this meant for internal auditors was that for two to three years, the only auditing they did was related to Sarbanes-Oxley compliance, documenting and testing financial reporting and disclosure controls.[7]

Sarbanes-Oxley brought many benefits to the profession of internal audit. Overnight, internal auditors went from relative obscurity to center stage.[8] Organizations saw in the internal audit function the capacity to meet the compliance requirements of Sarbanes-Oxley. However, as companies transition the Sarbanes-Oxley effort from a project to an institutionalized process, the role of internal auditors is again in a state of transition. It is not yet altogether clear what that future role will look like. Doubtless, like the debate over financial audits or operational audits, it will depend more on the individual company. The danger to the internal audit profession is that it will not change and adapt to the changing environment, needs, and circumstances, and that once again—like that adaptation to the standard business model—internal audit will stop evolving in terms of how it meets the control needs of the companies. While the objectives of internal

control have remained the same since the days of the Mesopotamian and Egyptian empires, the approach to achieving those objectives must adapt and change.

5.3 THE ROLE TRANSFORMED

Control validation (i.e., testing) illustrates this adaptation process. Sampling and sampling methods have undergone and will continue to undergo change. These changes do not invalidate the earlier approaches, which still have their uses, but they do, however, evolve the practice of internal audit, making it more effective and more relevant to companies.

Years ago, internal auditors made sample selections to evaluate attributes of a population of transactions. (See Exhibit 5.1.) Sometimes this selection was made statistically, sometimes through judgment. The goal was to have a representative sample so that a valid conclusion could be made about the population.[9] As new tools became available and more data was stored in accessible electronic formats, internal auditors queried and analyzed the transactions with the purpose of finding trends or attributes that might indicate errors in processing or other items significant to the control objectives being evaluated. In this way, there was less need to test transactions that were processed correctly. Internal auditors could instead focus their audit efforts on those transactions with at-risk attributes. Another benefit to this approach was that the entire population could be examined, not just a small sample.

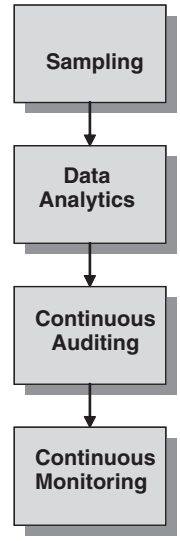


EXHIBIT 5.1 TESTING EVOLUTION OVER TIME

Over time, it became apparent that if internal auditors could run queries and analyze transactions to identify the at-risk transactions during audits, there really was no need to wait for an audit. Instead, this review could be done continuously as the transactions were being processed, highlighting the at-risk transactions when they occurred and not simply at the next audit cycle. This continuous audit approach is one that many audit departments are now beginning to embrace.[10] Some argue that annual audits are continuous auditing, just with an annual cycle. Depending on the risk characteristics of the attributes being evaluated, an annual cycle may be the right choice. In other situations, a real-time evaluation may be more appropriate.

The goal of continuous auditing is twofold: first, to deploy scarce internal audit and management resources more efficiently by searching for and looking at the problems, not the transactions that are working well; second, to identify at-risk transactions as soon as possible for early intervention, keeping problems to a minimum. These advantages of continuous auditing have gained the attention of audit committees, who now expect internal auditors to use these techniques.[11]

The next stage of evolution in this cycle is continuous auditing and continuous controls monitoring (CCM), which results in information that identifies potential anomalies, risk exposures, and control breakdowns.[12] This information should prompt immediate attention, further investigation, and remediation, and Sarbanes-Oxley may very well become an important factor in the broad adoption of this change. Most companies required to comply with Sarbanes-Oxley recognize that the ownership of internal control belongs with management.[13] Continuous monitoring in essence takes continuous auditing and puts the at-risk transactions at the fingertips of management through the use of enabling technology. Previously, management waited for the audit results to know there was a problem, and then reacted to audit findings with corrective actions. The evolution of technology is such that today internal auditors can provide management the at-risk transactions in real time for ownership, response, and resolution.

For many years, the role of internal auditors has been focused on providing assurance services. A gradual shift occurred during the 1990s, and internal auditors now are also expected to provide advisory services.[14]

5.4 BEYOND ASSURANCE: ADVISORY SERVICES

Beyond compliance, another catalyst enhancing the role of internal auditors is the increase in stakeholder demands for advisory and consulting activities. Discussions within the IIA to determine the nature and extent of these activities and whether internal auditors should perform such activities began in the 1990s and in many ways continue today. Advisory and consulting engagements are performed to capitalize on internal auditors' broad experience and their ability to identify process improvement opportunities without sacrificing the control environment. Regardless of the nature of their assurance or consulting activities, internal auditors are expected to act with independence, objectivity, and due professional care. High levels of financial, accounting, information technology (IT),

and business analysis expertise are typically required to perform these duties, in addition to being able to recruit, manage, and develop talent, communicate effectively, build relationships, lead others effectively, work collaboratively, and have a broad business experience.[15]

The role of internal auditors has also been impacted by the increase in organizational restructurings, mergers, and acquisitions; the rising complexities in finance and accounting; and globalization. The changes caused by globalization, increased government regulation, relentless competition, and the high mobility of investment capital challenge internal auditors to increase their technical competence in many ways. It is not unusual for internal auditors to be required to learn about information technology, business continuity planning, system access, physical security, and e-commerce. This changing landscape affects captive (i.e., in-house) and merchant (i.e., outsourced) internal auditors alike. Whereas a few decades ago, business activities were relatively predictable and focused on particular segments (e.g., manufacturing, retail, transportation), the advent of the conglomerate in the 1970s and the multinational more recently has increased the size and complexity of organizations. Most organizations typically outsource portions of their operations, respond to various exposures through derivatives and contracting arrangements, may own subsidiaries unrelated to their core business to diversify the revenue stream, and, when publicly traded, must meet ever-increasing performance expectations and regulatory scrutiny.[16] As a result, what constituted a relatively straightforward supply chain or treasury review in the past is now a rather complex endeavor.

As much as the technical challenges have increased, so have the nontechnical requirements of auditors. The soft skills needed often include the ability to speak foreign languages, function in diverse cultures, act as facilitators during group sessions, and provide training to process owners. It is common for audit teams to consist of individuals who grew up in different countries, speak different languages, have different academic backgrounds, and operate on different value systems and traditions. For these teams to be effective, internal auditors must collaborate, compromise, and motivate and appropriately reward performance.

The prevalence of virtual audit teams—administratively affiliated with one or a few offices but physically scattered around the world, performing audits and special projects—has also created various challenges. For many audit departments, creating and maintaining a sense of community and keeping travel requirements to manageable levels can be difficult. While the new dynamics and expectations create some unique managerial challenges, they also create some tremendous opportunities for companies. Internal auditors are well positioned to learn about best practices around the organization that they can then share with other locations. They identify risks and opportunities, bring them to management's attention for appropriate action, and make recommendations that factor in unique circumstances unknown to many other parties.

Today's internal auditor must act as an educator, technical resource, competent manager, process analyst, and strategic thinker. These duties require strong leadership qualities, superb communication skills, and the ability to build relationships; have an impactful presence; and collaborate with various stakeholders within and outside the organization. Other required skills are the ability to provide ethical leadership, practice a healthy skepticism, have a global perspective, possess expertise in matters regarding governance, and be technologically competent.[17]

The focus of internal audit must be to act as a strategic partner and contribute ideas that help make the organization's vision a reality. To fill this role, internal auditors must possess the business acumen to provide guidance and actionable strategic recommendations, and must be constantly alert to emerging trends and communicate these changes to the organization's leadership. The internal auditor must counsel and advise in matters that others sometimes overlook.[18]

When internal auditors deliver value-added assurance and advisory services, they will achieve legitimacy within their organizations. Legitimacy, once attained, must be protected and enhanced through the careful, competent, and consistent execution of value-added internal audits. This process is further aided by the presence of a board-approved charter that ensures the internal audit function has the technical, human, and monetary resources needed to hire and train its auditors. The charter should guarantee access to all employees and the resources necessary to carry out the function's duties, and provide unfettered access to the audit committee of the board of directors.[19]

5.5 ACHIEVING THE GREATEST IMPACT

Internal auditors are uniquely positioned to help management achieve organizational goals by adopting a risk-based audit approach that is focused on the areas where exposures represent the highest significance and likelihood. Proactive auditors will also look for the dependencies that management's strategic objectives have—that is, supplement analyzing the risk of adverse events with the identification and management of events that must go well so that the organization's objectives can be achieved. Rather than merely focusing on what can go wrong, internal auditors can enhance management's ability to achieve its objectives by helping management determine what needs to go right and identify critical success factors. Furthermore, risk assessments should not be limited to the identification of risks, but should also help identify opportunities, determine the organization's preparedness, and identify those parties responsible for appropriately responding to those events. This risk assessment and response matrix can serve the organization well and increase the likelihood that goals and objectives will be achieved. In today's highly competitive business environment, organizations lacking the ability to adapt could be as likely to fail as those that poorly manage the risk of adverse outcomes.

Another key contribution internal auditors can make is to include recommendations for improvements in operations and procedures with their control recommendations. This can be accomplished by closely examining or even questioning the appropriateness, usefulness, and relevance of policies and procedures, which have a tendency to become outdated. Internal auditors should quantify the potential savings or cost reduction when making recommendations and balance the goal of verifying the presence of sound controls with the goal of efficient and effective operations.

Internal auditors can add value by helping their organization implement a framework of internal control and governance such as COSO's Enterprise Risk Management (ERM). This model's eight components encompass the organization's internal environment, its objectives, the identification of risks and opportunities, risk assessment, risk response, related control activities, information and communication, and a monitoring function to ensure the process is in place and working as intended. ERM can help management achieve the organization's performance and profitability targets, while preventing the loss of resources by aligning the risk appetite with its strategy. Other benefits of ERM include improving the quality of risk response decisions, reducing operational surprises and losses, facilitating the adoption of a portfolio view of risk, and improving the deployment of capital.[20]

Another area where internal auditors are often called upon to assist management is the development of antifraud programs that will codify the organization's fraud deterrence, prevention, detection, and investigation efforts. The proliferation of electronic transactions and the complexities of business activities create conditions that sometimes make organizations more vulnerable to fraud. Misappropriation of assets, corruption, and fraudulent statements are costly and very difficult to detect.[21] This condition is not isolated to a few countries, but is rather a global problem.[22] In this environment, internal auditors must have sufficient knowledge to identify fraud indicators. In fact, the IIA states, "The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud" (International Standards for the Professional Practice of Internal Auditing 1210.A2).[23] In many cases, internal auditors develop an expertise in forensics, investigating instances of fraud and assisting law enforcement officials. Internal auditors can play a key role in helping organizations focus on fraud deterrence and prevention, training employees and verifying that fraud risk assessments are performed routinely. This proactive stance is an improvement on the reactive approach many organizations have to fraud, where they focus disproportionately on detection and investigation.

Today, a wide variety of data resources provide benchmarking data and analysis of financial and operational data for comparison and the identification of trends, concentration, and apparent anomalies. This information is often available online, free or by subscription, making it possible for internal auditors to gauge

performance and identify areas requiring further review. Other tools now available include work paper management software, programs to perform data analytics, and applications that allow the monitoring of activities and the creation and management of an audit trail of transactions.

Reporting audit observations is a key requirement for internal auditors, and beyond identifying problems, management expects internal auditors to provide timely, useful, relevant, and feasible recommendations. When tailored to the organization and integrated with the input of key management personnel, these recommendations should in fact be agreed-upon action items that will add legitimacy and relevance to the audit function. Improvements are often found by consciously seeking opportunities to reduce cycle times, eliminate rework, introduce paperless processing, and integrate processing systems, and by performing benchmarking studies within and outside the organization. These activities can align what internal auditors do with the organization's imperative to operate more efficiently and effectively. (See Exhibit 5.2.)

Internal auditors can expand their coverage by helping to train staff within the organization to meet these challenges and provide value-added services. Internal audit departments must be funded sufficiently to carry out their duties as documented in the charter. They should also have the resources necessary to perform special projects that from time to time are required of them. Their ability to do so will be founded in their proficiency and competence and presupposes continuous training and development. Constantly updating skills and keeping pace with operational and IT changes are imperative for success.

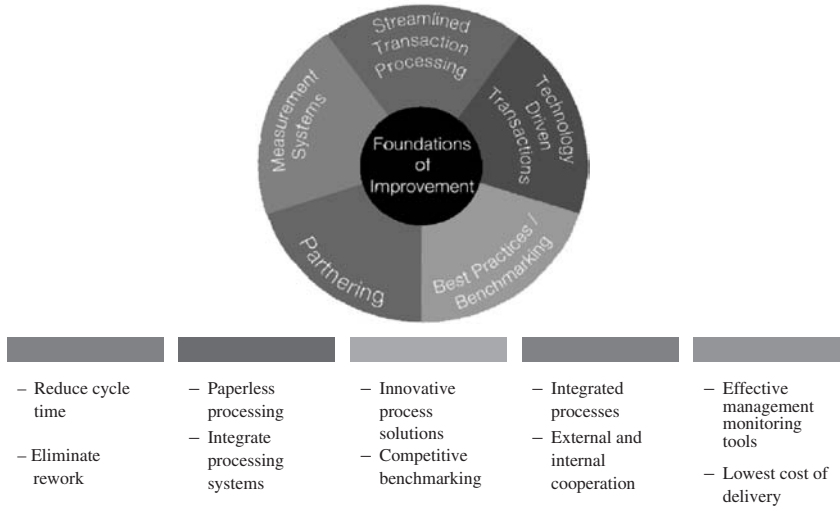


EXHIBIT 5.2 FOUNDATIONS OF IMPROVEMENT™

5.6 THE BRIGHT OUTLOOK OF INTERNAL AUDITING

As these changes take place, internal audit will become less focused on finding problems and more focused on acting as control design consultants. In this environment, internal auditors will:

- Help management design systems of internal control that can be monitored efficiently
- Assess the continued effectiveness of the monitoring process in ways that are less resource intensive than trying to find the problems
- Evaluate the effectiveness of management controls that cannot be tested with technology
- Identify opportunities to reduce risk and improve the organization's chances of meeting its stated business objectives

This future state will challenge internal auditors to balance their testing of quantifiable hard controls with subjective intangibles such as the ethical climate, the integrity of management, the competence of employees, and the ethical environment in organizations.[24] In addition, controls are increasingly IT dependent and will require internal auditors to complement their traditional accounting, financial, and operations skills with the ability to act as business analysts. For example, achieving CCM's full potential requires identifying automation opportunities and writing software scripts and programs to collect, analyze, and report on relevant data for appropriate action. While internal auditors are unlikely to replace software developers anytime soon, they will be required to liaise between process owners and those who will perform these highly technical duties. Internal auditors' extensive knowledge about their organizations' processes, control structures and environments, and corporate objectives and risk factors makes them uniquely qualified to act in a pivotal role, helping to facilitate this transition to continuous monitoring. Their role as providers of assurance and advisory services will be greatly enhanced by helping organizations adopt continuous monitoring initiatives to provide timely and actionable information that can be acted upon before festering problems cause regulatory, financial, or operational crises.[25] As the role of internal auditors grows and becomes more complex, it also creates exciting career and learning opportunities; in fact, the demand for auditors is very strong.[26] For those who embrace this challenge, the prize will be that investors, regulators, boards of directors, management, and the public at large will continue to view internal auditors as valuable, relevant, useful partners whose deliverables are timely and actionable.

Notes

1. For the complete definition of internal auditing, see the introduction to the International Standards for the Professional Practice of Internal Auditing at the Institute of Internal Auditors (IIA) web site, www.theiia.org/?doc_id=1499.

2. Lawrence Sawyer, *Sawyer's Internal Auditing: The Practice of Internal Auditing* (Altamonte Springs, Florida, 1988). Sawyer provides a history of the evolution of internal auditing. For a summary of significant events in the IIA's history and the growth in its membership, see www.theiia.org/index.cfm?doc_id=4929.
3. Sawyer, *Internal Auditing*.
4. Ibid.
5. For additional information regarding this transformation, see Sue Gilly, *The Development of Management* and Organizational Thinking (1997) at http://home.flash.net/~jteague/Sue/dmot.htm.
6. Ibid.
7. Many articles have been written on the cost of complying with the Sarbanes-Oxley Act of 2002. Some of these articles are found in the *Economist* (May 19, 2005), *USAToday* (October 19, 2003), the *CPA Journal Online* (November 2004), *Internal Auditor* (December 2003), *Sarbanes-Oxley Compliance Journal* (October 6, 2005), and *Compliance Week* (October 18, 2005).
8. For additional information regarding the job requirements and career prospects of internal auditors, see the U.S. Department of Labor at www.bls.gov/oco/ocos001.htm, Manpower's *2005 Salary Survey Report* at www.manpower.com/mpcom/files?name=MP_salarysurvey_Accounting.pdf#search=%22salary%20survey%20internal%20auditor%22, *Internal Auditor*'s June 2006 special feature story "Special Section: Training/Recruiting and Salary Survey," JobBankUSA at www.jobbankusa.com/career_employment/accountants_auditors/training_certifications_skills_advancement.html, and the AICPA at http://www.aicpa.org/nolimits/job/paths/index.htm.
9. Techniques for effective research design and sample selection are discussed in: A. Fink, *The Survey Handbook*, 2nd ed. (Thousand Oaks, CA: Sage Publications, 2003). R. Yaremko, H. Harari, R. Harrison, and E. Lynn, *Handbook of Research and Quantitative Methods in Psychology: For Students and Professionals* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1986). P. Martin and P. Bateson, *Measuring Behavior: An Introductory Guide*, 2nd ed. (Cambridge, UK: University Press, 1993).
10. Eighty-one percent of companies surveyed reported that "they either had a continuous auditing or monitoring process in place or were planning to develop one" (PricewaterhouseCoopers, *2006 State of the Internal Audit Profession*).
11. Richard Chambers, "How Continuous Audit Improves Compliance," *Business Finance* (March 2006).
12. See "IIA Releases GTAG Guidance on Continuous Auditing," published in the IIA's *CAE Bulletin* (October 12, 2005) at www.theiia.org/CAE/index.cfm?iid=410; the Office of Management and Budget (OMB) Circular No. A-123 at www.whitehouse.gov/omb/circulars/a123/a123_rev.html; ACL's white paper entitled "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment" at www.acua.org/pdfs/ACLWhite.pdf; and "Continuous Auditing on the Rise" in the August 2006 issue of *Internal Auditor*.
13. See *Internal Control—Integrated Framework Executive Summary* at www.coso.org/publications/executive_summary_integrated_framework.htm and *Compliance Week* (October 18, 2005) at www.complianceweek.com/index.cfm?fuseaction=article.viewArticle&article_ID=2081 for additional information regarding management's role in the management and ownership of the system of internal control.
14. See the IIA's definition of internal auditing, which makes reference to the consulting activities that internal auditors perform, at www.theiia.org/index.cfm?doc_id=123. The

articles "Consultant Auditing Charting a Course" in the December 2001 issue of *Internal Auditor* and "The Audit Profession: Center Stage" in the April 2003 issue provide insightful reviews of consulting in the internal audit profession.

15. See Korn/Ferry International's "Talent Requirements for Internal Audit and Compliance Executives," presented at the Information Technology Association of America conference on April 6, 2004, available at www.itaa.org/software/events/presentations/998.ppt.
16. Some examples of these regulatory requirements include the Sarbanes-Oxley Act of 2002 in the United States and similar legislative acts in other countries (e.g., MI-52/Bill 198 in Canada, La Loi de Sécurité Financière (LSF) in France, and J-SOX, the unofficial term for Japan's equivalent of the Sarbanes-Oxley Act, Sections 302 and 404.
17. Korn/Ferry, "Talent Requirements."
18. Ibid.
19. The IIA provides samples of internal audit department and audit committee charters on its web site at www.theiia.org.
20. For additional information about COSO and COSO ERM, see *Internal Control—Integrated Framework* and *COSO ERM Framework* (September 2004) at www.coso.org.
21. The *ACFE Report to the Nation on Occupational Fraud & Abuse 2006* from the Association of Certified Fraud Examiners at www.acfe.com/documents/2006-rttn.pdf provides an in-depth review of fraud.
22. Transparency International (www.transparency.org/) publishes various surveys and indexes such as the Corruption Perceptions Index, the Global Corruption Barometer, and the Bribe Payers Index. The World Bank publishes various research papers on fraud and corruption through its Investment Climate Research Program, and the United Nations has various publications addressing corruption through its Office on Drugs and Crime. The larger accounting firms conduct similar research and issue their findings in reports such as *PricewaterhouseCoopers' Global Economic Crime Survey 2005*.
23. Other entities requiring auditors to possess antifraud knowledge or implement antifraud programs include the Sarbanes-Oxley Act of 2002 (Section II(B)(3)(d)), PCAOB Auditing Standard No. 2 ¶139, Statement of Auditing Standards No. 99—Consideration of Fraud in a Financial Statement, and the U.S. Federal Sentencing Guidelines §8B2.
24. See Curtis Verschoor's "The Ethical Climate Barometer" in the October 2004 issue of *Internal Auditor*, David Sinason's "Auditing the Ethical Environment" in the November/December 2005 issue of *Internal Auditing*, Colleen Waring's "Measuring Ethical Climate Risk" in the December 2004 issue of *Internal Auditor*, and Colleen Waring and C'Anne Daugherty's "Auditing Ethics" in the Spring 2004 issue of the *Journal of Government Financial Management* for useful suggestions for auditing the ethical environment.
25. Anne Lawrence, James Weber, and James Post, *Business and Society: Stakeholders, Ethics, Public Policy*, 11th ed. (New York: McGraw-Hill Irwin) provides additional information about the avoidance of crises through early intervention and the nurturing of effective stakeholder relations.
26. For additional information regarding the increasing demand for auditors and career opportunities in internal auditing, see the articles "Boom Time for Internal Audit Professionals" and "The Quest for Talent" in the June 2006 issue of *Internal Auditor*. The U.S. Department of Labor Bureau of Labor Statistics indicates "An increase in the number of businesses, changing financial laws and regulations, and greater scrutiny of company finances will drive faster-than-average growth of accountants and auditors" in the *Occupational Outlook Handbook* available at www.bls.gov/oco/ocos001.htm.

CHAPTER 6

OUTSOURCED PROCESSES: RISK AND RESOLUTION

Mark Stebelton

6.1 A MATTER OF RISK

The objectives of a business are not to perform internal human resource operations. Nor is the objective to perform fixed asset analysis, receivables collections, or information technology (IT) support operations. The objectives of a business are to perform its core competency, whether that is manufacturing, media production, software development, distribution, or any other activity.

This is not to say those functions are not critical, important, or valuable; they are. But all these ancillary and extraneous activities are simply a necessary evil of being in business. The key word here is *necessary,* since without these functions, a business could not exist. Because of this, and realizing that expending energies in noncore areas detracts from focusing on the true objectives of their business, many organizations look to third-party service providers to fill those roles.

The benefits of third-party service providers are several-fold. Since the service being provided is the core competency of the third-party service provider, it typically invests in maintaining a proficiency in its respective service area, whether that is through resource training, technology, or any other area. An additional benefit is that many times these service providers can provide the necessary functions for equal to, or even less than, the cost for which an organization could perform the same functions in-house.

Along with these apparent benefits, there are significant risks that come along with the outsourcing. In the initial outsourcing determination and selection process, an organization must address three broad types of risks, says Ravi

Aron, Wharton professor of operations and information management and a leading authority on outsourcing trends:

1. *Operational risks* show up as slippages on time, cost, and quality. Professor Aron says these frequently arise with breakdowns in the transfer of work processes, or in repetitive processes that are prone to human error. He notes that operational risks do not arise from deliberate misbehavior; instead, they are most likely to occur when the service provider does not completely understand a client's requirements.
2. *Strategic risks* are rooted in deliberate, opportunistic behavior by service providers or their employees. Theft of intellectual property is the most common but far from the only example. Another type of strategic risk involves providers who cut corners by understaffing. A third is what Professor Aron calls an "asymmetry of dependence": "All goes well for three years, and when the contract comes up for renewal, the contractor doubles the price because he knows the client is locked in and it is not easy for it to switch suppliers."
3. *Composite risks* manifest themselves when a client company has outsourced a process for so long that it can no longer implement the process for itself, says Professor Aron. "For instance, over a period of eight to 10 years, a retail financial-services company may not have any back-office operational capabilities if all of its retail customers are managed by offshore contractors in Mauritius or Manila," he says. That could present problems when the client company has a new product and discovers that an entire set of needed in-house skills has eroded. Professor Aron adds that such risks have a relatively easy solution: Companies can retain minimal residual capacities so that they always have in-house access to outsourced skills.[1]

After these risks have been addressed and the decision made to outsource, the senior management team must address the compliance and regulatory risks that are inherent to any business process regardless of whether it is performed in-house—that being the risk of improperly calculating and reporting financial activities or obligations that are material to the financial statements. It is critical that senior management must have a clear understanding of what outsourced processes may have a material impact to their financial statements.

6.2 A MATTER OF RESPONSIBILITY

Once senior management has all of their material outsourced activity ducks in a row, several important questions surround the compliance and regulatory risks of outsourced activities. The first is: Who owns the risk? The second is: What are ways to mitigate this risk?

While many governing institutions address this topic, the common understanding is that the outsourcing organization retains the responsibility to properly

manage the risk related to the activities. The Committee of European Banking Supervisors (CEBS) reiterates this theme multiple times in its "Guidelines on Outsourcing."[2] The rationale is that management remains responsible for their financial statements and therefore any inputs into those financial statements remain management's responsibility as well, regardless of their origin.

Under the Sarbanes-Oxley Act of 2002 (SOX) Section 404, organizations are responsible for ensuring that the service providers of any outsourced functions have documented their financial processes, carried out a risk assessment, and put in place adequate controls over financial reporting that have been thoroughly tested for effectiveness. This responsibility cannot be delegated to the service provider by the organization.

However, this issue is not specifically related to Sarbanes-Oxley, as in 2000 the Board of Governors of the Federal Reserve System released SR00-4, "Outsourcing of Information and Transaction Processing," in which it states that the Federal Reserve expects institutions to "ensure that controls over outsourced information and transaction processing activities are equivalent to those that would be implemented if the activity were conducted internally."[3]

6.3 OUTSOURCED RISK MANAGEMENT

Now that the question of who owns the risk has been addressed, the next question is: How can management gain the proper degree of comfort that their outsourced risk is at an acceptable level? Several options exist; the outsourcing organization can have its own internal or external auditor conduct routine audits of the service provider, or the service provider can have its own external auditor provide audit reports to its user base.

If management has sufficient control over their outsourced service provider, they may need to take a more active role in the risk and control assessment activities of that service provider. This would entail utilizing their own internal or external auditors (or both) for a review and assessment of the service provider's activities as an extension of their own operations.

There is a downside to this from the perspective of both organizations. For the user organization, the additional resource cost can be quite significant and the logistics and timing difficult to manage. The service provider most likely will have multiple customers of its services and would therefore not be able to accommodate each customer with its own request for audit, as the support of such requests would negatively affect the provider's operational abilities.

The current solution to this is for the service provider to provide a standardized audit report for all of its customers to use in their assessment of risk. This is commonly referred to as an SAS 70 audit, from the Statement on Auditing Standards number 70, Service Organizations, an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).

An SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of its control activities, which generally include controls over information technology and related processes. In addition, an SAS 70 service audit is accepted under SOX in relation to Section 404.

However, this statement is somewhat misleading. A more accurate perception may be as Jabulani Leffel described it: "Since Sarbox [Sarbanes-Oxley] offers no guidance about how to audit outsourced controls services provider, the standard has become the de facto guideline for auditing the outsourced service concerns of publicly traded companies."[4]

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. An SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of an SAS 70 examination.

There are two types of service auditor's reports: Type I and Type II.

A Type I report includes the service organization's description of controls at a specific point in time (e.g., December 31). A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six-month period (e.g., June 30 to December 31). The contents of each type of report are described in Exhibit 6.1.

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

Report Contents	Type I Report	Type II Report
1. Independent service auditor's report (i.e., opinion)	Included	Included
2. Service organization's description of controls	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests	Optional	Included
4. Other information provided by the service organization	Optional	Optional

EXHIBIT 6.1 SERVICE AUDITOR'S REPORT TYPES

In a Type II report, the service auditor will express an opinion on the same items (1) and (2) as in a Type I report, and also (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

6.4 SAS 70 CRITICISMS

As is usually the case, SAS 70 is not without its detractors. Auditors and other critics of the standard say SAS 70 is in need of a major overhaul. First of all, the Type I report doesn't even include an opinion on the effectiveness of the control environment. This is a mandatory aspect of the report if the outsourcing organization's external auditors are expected to rely on it. Then the fact that it is for a specific point in time rather than as an assessment of control over a period of time further diminishes external auditors' ability to rely on it for their own audit purposes.

Even the Type II report (which has an opinion and covers a period of time as opposed to a point in time) is not a guarantee of compliance with Sarbanes-Oxley. The timing of the audit might be out of sync with the client's reporting period. For example, if the audit is performed in June and the client's fiscal year ends December 31, there is a six-month gap in the attestation of the outsourcer's internal controls. If the controls slip up during the second half of the year, the accuracy and reliability of the client's own year-end attestation could be compromised. This would increase the risk of a Securities and Exchange Commission inquiry. One response to the timing issue is to request that the service provider undergo SAS 70 audits on a quarterly basis with updates throughout the year.

Another concern for the outsourcing organization's external auditors relates to just how much of the service provider's audit is being revealed. A service provider is required to inform its client only about any failures of SAS 70 tests; there is no requirement to spell out the exact scope of the audit.

This leads into a critical discussion of how an SAS 70 audit does, or does not, address information system security. Jabulani Leffel brings up some interesting points in his article related to SAS 70: arguing that the purpose of the standard is widely misunderstood, especially as to what technology areas are covered in an audit. "An SAS 70 is intended to be a service-auditor-to-client-auditor communication tool. But some [information technology] people think it affirms privacy and security. It doesn't," says Everett Johnson, president of the Information Systems Audit and Control Association in Rolling Meadows, Illinois.

For instance, at a company like Vengroff, Williams & Associates, a service group that handles receivables processing for its clients, an SAS 70 would cover only business-process controls pertinent to the revenue cycle. It would not necessarily cover other areas, like IT, as extensively as a client and its auditor might think.

Gabe Torek, Vengroff's chief information officer, says that having an SAS 70 to review is important for corporate clients seeking services. "But by no means does it eliminate due diligence," he said. "If you're depending on SAS 70 for assurances around information security, you're depending on the wrong thing."[5]

The flip side to all this can be seen when Jennifer Bayuk, managing director of IT security at Bear, Stearns & Company, is quoted in an article on SAS 70 by Michael Fitzgerald as saying that an SAS 70 audit is "probably the best you can get for a security test, especially when you compare it to something like a security penetration study."[6]

6.5 SAS 70 ALTERNATIVES

While there is no specific alternative to SAS 70 from a SOX perspective at this time, senior management with a low tolerance for risk around their outsourced activities may begin requiring additional compliance by their service providers to other standards such as ISO 17799 or CobiT. These other standards would be in addition to SAS 70, as a supplement rather than replacing SAS 70 altogether. In fact, if anything, more organizations that previously relied exclusively on these other standards are turning to SAS 70 as a requirement.

In actuality, as evidenced by the dichotomy of opinions related to the existing guidance, it is apparent that new guidance is required. As the Public Company Accounting Oversight Board (PCAOB) updates AS2 and as the Securities and Exchange Commission issues clarifications to Section 404, there is the hope that SAS 70 will evolve or that a new standard will be implemented to replace SAS 70 and more clearly articulate the necessary requirements.

Finally, one additional thing that SAS 70 does not address is the transition point (handoff) between the outsourcing organization and the service provider. It remains the sole responsibility of the outsourcing organization to both control and assess. These transition points are often overlooked by senior management until they come up as issues during an audit.

6.6 SUMMARY

As organizations actively look for ways to decrease costs of their operations, outsourcing of noncore business processes will continue to be a viable alternative. Most of these processes will have a material effect on the outsourcing organization's financial statements and will therefore be under the same risk and assessment requirements as its in-house processes. For SOX (Section 404) and for other regulatory and compliance standards, these risk and assessment responsibilities remain with the senior management of the outsourcing organization.

The intent of the SAS 70 is to provide management and the external auditors of the outsourcing organization the necessary understanding and comfort level with regard to the internal control environment surrounding the activities offered by the service provider. While it has several flaws related to the disclosure and

timing aspects of its performance, at this point it appears that the SAS 70 is the most viable and cost-effective option.

Notes

1. "Reining in Outsourcing Risk," Strategy-Business.com, www.strategy-business.com/sbkwarticle/sbkw051130?pg=all.
2. "Guidelines on Outsourcing," Committee of European Banking Supervisors (CEBS), December 14, 2006.
3. SR00-4, "Outsourcing of Information and Transaction Processing," Board of Governors of the Federal Reserve System, February 29, 2000.
4. Jabulani Leffel, "SAS 70 Weak on Data Security," CFO.com, November 27, 2006.
5. Ibid.
6. Jennifer Bayuk, quoted in Michael Fitzgerald, "SAS 70," CSO.com, December 2005, www.csoonline.com/read/110105/sas70.html.

CHAPTER 7

THE LAST MILE OF FINANCE

Eric Keller

If you navigate it properly, you can have a smooth financial close, a good set of internal controls, and an accurate set of financial statements.

Note: Some of this material was originally published in *Strategic Finance*, March 2006.

7.1 THE LAST MILE OF FINANCE

As I speak with today's CFOs and other senior finance executives and compare the challenges they face with the ones I tackled during my years as a public company CFO, it is apparent that the job has become increasingly difficult. In the past 25 years, an abundance of new accounting rules has been introduced at the same time that reporting deadlines have been compressed, requiring a more rapid close process. Sarbanes-Oxley (SOX) compliance has further added to these challenges, dramatically increasing the time and cost to ensure that financial statements are accurate, complete, and timely. Finally, increased regulatory scrutiny has resulted in lower materiality thresholds so that even relatively small errors in financial statements can result in material weakness disclosures or financial restatements.

Here are some tangible examples of these trends:

- During the past 10 years, a typical quarterly report (10-Q) to the Securities and Exchange Commission (SEC) has grown roughly fivefold—from 10 or 15 pages to 50 and 75 pages—reflecting an increase in both the number and the complexity of disclosures that public companies are required to make.

- Filing deadlines for submissions to the SEC are accelerating significantly: Large-company quarterly filing deadlines have been reduced from 45 to 40 days and annual deadlines from 90 days to 75, with further reductions likely.
- The number of public companies issuing restatements has also grown dramatically from 100 in 1997 to an expected 1,200 in 2005 as estimated by Glass Lewis & Company, an investment research advisory firm. In addition, approximately 15 of public companies disclosed material weaknesses last year.
- Audit fees for public companies are also on the rise. A June 2005 study by Foley & Lardner found that audit fees for a sample of more than 700 public companies increased from an average of $1.6 million in 2001 to more than $4 million in 2004. Small and mid-cap companies saw their audit fees almost double in 2004 alone.

For public companies, these trends—coupled with pressures to reduce staffing levels in the finance organization—mean mounting pressure on financial professionals. A *CFO* magazine survey asking more than 200 finance executives how their work had changed in recent years found that two-thirds felt that pressures on them were increasing and that work-related stress was taking a toll on their health. As a former CFO myself, I am no stranger to the grim statistics: Turnover in CFO positions in public companies is very high, as many have decided that the benefits of their jobs just don't outweigh the stresses and risks.

7.2 REGAINING CONTROL

Forward-looking finance executives aren't surrendering to these trends—they are looking for solutions that will help them produce accurate financial results in a shorter period of time while simultaneously sustaining SOX compliance and reducing costs.

The Public Company Accounting Oversight Board (PCAOB) recently recommended a number of steps to improve compliance and reduce inefficiencies associated with the initial year of SOX. First, the agency recommended that the audits of a company's financial statements and internal controls be integrated as a way to save time and reduce costs. This integrated approach allows the objectives of both audits to be achieved simultaneously, saving time and money and identifying issues before the financial statements are issued. Today, most companies still run the preparation of their financial statements and the work to demonstrate an effective system of internal control over financial reporting as separate processes, thus increasing the risk of both material weakness disclosures and restatements.

Second, in addition to emphasizing the importance of an integrated audit of the financial statements and internal controls, the recent PCAOB guidance

(Release 2005-023, November 30, 2005) stressed the importance of the quarterly financial reporting process:

> The period-end financial reporting process is always a significant process because of its importance to the company's financial reporting. The period-end financial reporting process ordinarily consists of a combination of manual and automated functions, requires considerable judgment to evaluate, and presents numerous opportunities for misstatements to occur. Given the high degree of risk that misstatements could occur during the period-end financial reporting process, significant attention to this process is necessary in virtually all audits.

At most companies, this period-end financial reporting process is known as the close. It encompasses all accounting processes and journal entries created by the finance team to accurately recognize and report the financial results and position of the company, and it includes the reporting of the statements and disclosures in SEC-required financial statements. The quarterly financial close is also a time during which auditors, controllers, CFOs, and compliance officers operate under enormous time pressures to detect exceptions and potential errors and produce financial statements that reflect the company's financial results fairly and in accordance with generally accepted accounting principles (GAAP).

The dual objectives of the integrated audit and improving the close process have created the concept of an integrated financial close in which financial controls and close tasks are linked directly to a company's financial statements, creating a system of record for both the financial close and financial compliance. Combining these activities reduces compliance costs, improves efficiency of finance teams and auditors, and enables everyone to focus their attention on exceptions, issues, and key risks.

John Verburgt, associate director of compliance at the Chicago Mercantile Exchange (CME), thinks that the move to assimilate compliance into financial close processes is self-evident. "Compliance should not be viewed as a separate process," he says. "Compliance is part of the way that we do business. Most of what is performed during a financial close is a control of ensuring our financial statements are accurate and reliable. What SOX has done is it has taught people a lot about their jobs and also doubled as a to-do checklist."

Despite the goal of an integrated financial close, most public companies currently lack a unified framework that allows them to successfully merge the critical processes associated with the quarterly financial close with their efforts around Sarbanes-Oxley compliance.

7.3 WHERE EVERYTHING COMES TOGETHER

Many of today's issues—from corporate governance to restatements and SEC filings—come to a head in what can be called the "last mile" of finance, the last critical phase of financial management prior to public disclosure where aggregated financial and operational information is turned into a set of financial statements.

The last mile of finance is the series of steps involved in the close from consolidation through the company's public disclosure of its financial results, including filings with the SEC. As most financial professionals have experienced, the process of preparing financial statements is fraught with risks, costs, complexities, and inefficiencies. Yet it is the final opportunity for finance departments, auditors, and audit committees to identify and address the issues or errors that could later result in a restatement.

The financial close and the SOX-related internal control tasks that make up the last mile are composed of a wide variety of interdependent activities supported by different technologies. Existing applications such as enterprise resource planning (ERP) and consolidation systems manage financial data and standard transaction processes, recording adjusting entries and aggregating quantitative information. But during the last mile, many of the most critical tasks required to produce accurate financial statements are performed manually, are often dynamic and analytical in nature, and frequently occur outside any formal systems of record.

The finance organization relies heavily on spreadsheets and other documents that are created and stored on personal computers throughout the company, and it frequently uses e-mail to informally communicate priorities, issues, and results. "Most close processes include an exhaustive list of activities to complete," Verburgt of the CME notes. "The toughest controls are the ones that are manually driven and where the most risk occurs."

Let's take the example of account reconciliations to discuss the manual processes in the close. An account reconciliation is the most fundamental of accounting controls and compares the summation of the details of an account to the total for that account in the general ledger. A reconciliation is a detective control that is performed on every material balance sheet account.

Although an account reconciliation is fundamental, that does not mean it is simple. One in five material weaknesses to date can be traced in whole or in part to issues related to account reconciliations. If you walk through the basic steps in the process, you will see the manual nature and potential risk of error with the account reconciliation process:

1. Locate an account owner. At most large enterprises, the addition of new accounts and change in personnel makes this step a clerical burden every quarter.
2. Extract the detail balance and general ledger balance to a spreadsheet. The errors in this step are related to version control and clerical errors.
3. Investigate and explain any material difference. This step contains a multitude of decisions, communications, and accounting steps that can be performed inaccurately.
4. Determine whether an adjustment is required. The personnel making these decisions may not be fully trained to understand whether an amount warrants adjustment, and reviews may be inadequate to catch the errors.

The reality at most large enterprises is that hundreds or even thousands of account reconciliations are performed each accounting period. At some corporations, this is pure drudgery and the exercise does not result in many adjustments; but at others, such as financial institutions with significant cash balances, the reconciliations are key controls that result in material adjustments. Account reconciliations are the bread-and-butter control in finance, and it is the sheer volume and manual nature of this work that is resulting in material weaknesses.

In addition to complexity, coordinating all these various activities and systems takes time, and, as noted earlier, filing deadlines are getting compressed. "In order to meet the new SEC filing schedules, U.S. companies must adopt strategic measures that will accelerate their financial reporting processes," Pat Neeley, Global Service Line lead of Parson Consulting, a leading financial management consultancy, says. "An effective way for companies to do so is to improve close processes now in a methodical way that is sustainable over time."

The most effective way to address these challenges successfully is to zero in on the last mile and embark on an automated close by bringing together the financial and compliance results from across the company. Conducting an effective integrated close means identifying and automating manual processes, linking information from ERP and consolidation systems, controlling the use of manual spreadsheets, and synchronizing compliance management with financial results to create reliable, accurate financial statements.

7.4 THE PATH TO AN OPTIMUM CLOSE

By implementing an automated, integrated close, a finance organization can combine the close for financial results and the assessment of internal controls with the overall financial reporting process to improve employee and auditor productivity, increase accuracy, and reduce audit costs associated with financial reporting. By automating the close activities and the SOX compliance testing, it is possible to integrate the two related processes and benefit from a more effective means to identify issues and a more efficient way to perform close and control activities.

Without an integrated close, or single close, the last mile is prone to several points of failure that increase corporate risk and cost. Missed close tasks or errors in disconnected spreadsheet-based analyses can lead to filing inaccurate financial statements, thus increasing the risk of material weakness disclosures and financial restatements (see Exhibit 7.1 for some material weakness examples). Without unified processes that highlight issues, finance spends time on unnecessary and inefficient processes rather than important analyses. And the lack of centralized, consistent documentation inflates audit costs. While other industries long ago turned to automation and efficiency, the work conducted by finance organizations in the last mile lags behind.

A single close is accomplished with an automated environment where control management and close tasks can be standardized, managed, and documented. Manual activities and spreadsheets can be controlled, tracked, and documented.

Problems in the ''last mile'' were frequently associated with material weakness disclosures during 2005, as demonstrated in the following excerpts from SEC filings.

Inadequate documentation of close process	''The company does not have sufficient policies and procedures related to the preparation of accounting records and the financial close, consolidation, and financial reporting processes.'' (eCollege.com, 10-K/A, May 2005)
Misstated accruals and expenses made during close	''The company concluded that controls over the financial statement close process related to the determination of accrued liabilities and prepaid expenses were not operating effectively . . . resulting in numerous adjustments.'' (The Princeton Review, Inc., 10-K/A, May 2005)
Breakdowns in the close process in international locations	''[T]he company did not have adequate procedures and controls to ensure that accurate financial statements [in] Europe can be prepared and reviewed by management on a timely basis.'' (Transkaryotic Therapies, Inc., 10-K/A, May 2005)
Inadequate controls over nonroutine transactions	''[A material weakness in the] design and implementation of adequate controls over the financial reporting and close process, including controls over nonroutine transactions.'' (General Cable Corporation, 10-K/A, April 2005)
Error in elimination of intercompany balances	''[W]e discovered an error in a spreadsheet application, which was designed to eliminate intercompany balances. As a result of the error, amounts accumulated in the property account for one subsidiary were inadvertently not eliminated in consolidation.'' (Edge Petroleum Corporation, 10-Q/A, March 2005)
Reliance on manual processes	''[T]he company did not maintain effective controls over the communication among operating, functional, and accounting departments of financial and other business information that is important to the period-end financial reporting process, including the specifics of nonroutine and nonsystematic transactions. Contributing factors included the large number of manual processes utilized during the period-end financial reporting process and an insufficient number of accounting and finance personnel.'' (Pride International, Inc., 10-K, March 2005)
Account reconciliation maintenance	''The company did not maintain effective controls over certain general ledger account reconciliations and the monitoring and review of general ledger accounts. Specifically, general ledger account reconciliations involving cash, receivables, income taxes, property and equipment, other current and noncurrent assets, payables, accrued expenses, notes payable, and other noncurrent liabilities in the United States, Mexico, and United Kingdom were not properly performed on a timely basis and reconciling items were not timely resolved and adjusted as well as a lack of monitoring and review of these general ledger accounts.''

Exhibit 7.1 Material Weakness Examples

Control testing and close task processes can be analyzed and issues addressed immediately. This means formalizing close activities, managing approved close spreadsheets, assessing key controls, increasing visibility of internal activities, and accomplishing this through a system of record that manages all the numbers, analyses, comments, and issues. A single close means dramatically reducing both external and internal costs as well as the risks that ultimately manifest themselves in material weakness disclosures and restatements.

Here are the essential elements of a single close:

- *Automate close tasks.* Rather than tracking the close manually, use work flow and automatic scheduling to guide close tasks to completion and issues to resolution. Advanced error-detection capabilities highlight problems and remove bottlenecks.
- *Manage approved close spreadsheets.* Ensure that financial personnel use preapproved spreadsheets to perform critical calculations such as reserves, intercompany eliminations, and asset valuations. Unmanaged spreadsheets frequently introduce inaccuracies and errors into financial results and often are the source of material weaknesses in controls.
- *Assess key controls.* Determine the operating effectiveness of key controls for all high-risk financial statement accounts by evaluating controls that are explicitly mapped to specific financial statement accounts that in turn are mapped to disclosures and reports. This explicit mapping of controls provides confidence in the accuracy and precision of financial statement account balances and, ultimately, in disclosure documents.
- *Increase transparency.* Whether the company performs a distributed or centralized close process, provide managers with a clear status for critical close tasks, including compliance activities, at any time during the close cycle to bring together the components creating a single close. Management consoles that provide a summary view of the close and drill down to details are indispensable.
- *Deliver an online close binder.* Use a software application that automatically creates an online close binder for the single close for each period. Providing this to auditors significantly reduces the time and money spent preparing for and supporting them and decreases the amount of work they must perform.

It's also a good idea to have a checklist for the finance team to use to make sure they have followed all the appropriate steps and procedures during their last mile walk.

7.5 A RETURN TO GOOD FINANCE

Good financial practices don't make headlines. It's the mistakes, the missed earnings, the scandals, and shots of CEOs and CFOs in courtrooms that make the news. Wouldn't it be nice if a newspaper or magazine celebrated or, at the very

least, acknowledged the hard work and effort that go into getting the numbers right? Not all mistakes are a scandals waiting to be found—some are just the result of too much complexity and too many moving parts.

Moreover, all the work on compliance hasn't been wasted. As the CME's Verburgt emphasizes, "We learned a lot during year one of SOX—it was an extremely challenging time. And what we realized is that implementing controls in our financial close processes helps us prevent and detect errors and exceptions. By bringing the two processes together, we have minimized any additional effort for our auditors and financial managers for sustaining SOX compliance. Rather, we've made the process more streamlined and efficient."

The role of finance is to help companies achieve their strategic goals and create value for shareholders, not to be merely a compliance enforcement organization. To do this, financial executives must be able to embrace their broader role in their respective companies—as trusted business advisers and strategic thinkers who contribute to the legitimate success of the enterprise. When controls are integrated into standard financial close processes, the focus of time and resources can shift from primarily compliance and return to a more balanced approach that includes helping organizations grow profitability and successfully.

Addressing the inefficient, disorderly state of the financial close and the increased needs of disclosure means getting down to the bread and butter of a financial team—their ability to interpret, analyze, and smartly evaluate the numbers. Producing a streamlined and accurate financial statement that will be used by the public to judge their company's financials is a complicated task and means adapting to a modern world—where other aspects of business are already running at full throttle. So, what are we waiting for? It's time to bring finance up to speed by applying today's technology to implement a single close in your organization.

CHAPTER 8

U.S. STOCK OPTION BACKDATING SCANDALS

Anthony Tarantino, PhD

8.1 INTRODUCTION

In all employer-employee relationships, there exists a classical dilemma in how to align the interests of both parties. This is sometimes known as the principal-agent problem and explained in detail in Professor Vinod Hrishikesh's "Fraud and Corruption" chapter (Chapter 9). The traditional means to align these two interests include wages, profit sharing, bonuses, and commissions. The goal is to tie the employee's compensation to the employer's well-being. Although they have been around for over half a century, stock options have become a popular vehicle only in the past decade as a great means to align the two interests, to preserve a company's cash, and promote long-term employee loyalties. Stock options have been promoted over the past 20 years as a reform to what was viewed as excessive executive compensation. Unfortunately, in practice stock options have not always been implemented as designed. The major scandals unfolding in the United States involve the backdating of option grant dates to the point most favorable to the recipient—defeating the purpose of tying compensation to performance.

Over 200 U.S. companies have conducted internal reviews of the option practices over the past two years. Academic studies, which were widely publicized by the press, demonstrated that option grant dates often occurred on days in which stocks were at their lowest levels for a given period. Mathematicians effectively argued that the odds of this being a coincidence were beyond the

realm of possibility. Many of the internal reviews found that option grants were misdated. This forced many companies to restate financial results going back as many as five years in that the grant prices were below the market prices reported for the grant dates.[1] The Securities and Exchange Commission (SEC) and the Federal Bureau of Investigation (FBI) are investigating over 140 companies for improperly reporting option grants and for other actions to mislead security holders about option grants.

Many U.S. companies have not been able to file their 10-Ks and 10-Qs because of difficulties in determining the correct compensation charges related to stock options. Some companies have even been compelled to delist over this issue. According to Weil, Gotshal, and Manges, LLP, the failures to file or delays in filing also "may violate covenants or representations or warranties in debt instruments, presenting a risk of default (and in some instances have produced declarations of default by lenders), may disable the company from satisfying in a timely manner regulatory requirements relating to financial reporting or other aspects of their business, and/or may disrupt key license, joint venture, or other business relationships for which current SEC reporting or financial statements are required."[2]

The term *backdating* has come into prominence because of the large number of internal investigations, regulatory actions, and criminal prosecutions under way. Ironically, there is no precise legal definition of backdating, which has also been referred to as "spring-loading" and "bullet-dodging." According to Weil, Gotshal, and Manges, LLP, these practices can be described thus:

- *Backdating* typically refers to the selection of a grant date with the benefit of hindsight so that the date is earlier than the date the grant was approved (mainly on a date when the market price of the shares to be acquired pursuant to the option was lower than on the approval date), with the result that the option when issued has intrinsic value (i.e., an exercise price below the prevailing market price, contrary to explicit or implied representations that the option was issued only at the market price).
- *Spring-loading* typically refers to the practice of granting options in anticipation of the disclosure of material information that is expected to produce an increase in the market price of the shares to be acquired pursuant to the option (i.e., under circumstances where it is intended that the options will in fact have intrinsic value).
- The corollary practice of *bullet-dodging* has also been identified, which involves the intentional setting of an option grant date after the approval date so that material information that is expected to cause a decrease in the market value of the related shares can first be disclosed, or the intentional timing of option grants so as to follow the release of material information of such nature, in either case with the result that the exercise price will reflect the market's reaction to the information and

be lower than it otherwise would be. Arguably, both spring-loading and bullet-dodging are inconsistent with an explicit or implicit representation that only "at-the-market" options have been issued.[3]

Contrary to popular belief, it is not illegal or unethical to issue stock options with an exercise price that is less than the market price if the following conditions are met:

- The issuance complies with the terms of the stock option plan approved by the shareholders (including representations about pricing at the market, if any).
- The issuance is properly approved, disclosed, and accounted for.
- The appropriate income tax treatment for such so-called discount options is applied.[4]

The scandals have come about for those companies that failed meet these conditions. In some cases, problems have arisen from confusion as to how to comply. In other cases the intent was clearly to circumvent the regulations.

8.2 THE PROS AND CONS OF STOCK OPTIONS

The debates over the cost versus benefits of stock options go back many years and can be summarized:[5]

- *Pro:* Stock options do not require cash, which is critical to many cash-strapped start-up companies that may not yet be profitable. More shares issued dilute the losses per share.
- *Pro:* The holder does not have to declare any taxable income until the options are exercised, and the tax is calculated at a lower capital gains rate and not as income. *Con:* This provides an unfair tax advantage over other taxpayers.
- *Pro:* Issuing actual shares instead of options would cause a dilution of earnings and voting control. *Con:* The shares' costs would be known and then recorded as an expense.
- *Pro:* Options provide loyalty incentives to employees as stock prices rise. *Con:* When stock prices fall, employees have no incentive to work hard or remain with the company.
- *Pro:* Options align the interests of employees, the company, and shareholders. *Con:* The company has incentives to repurchase shares rather than paying dividends; no dividends accrue to the options.

8.3 THE AMERICAN SCANDALS

In 2005 and 2006, the backdating of stock options emerged as potentially one of the largest scandals in recent history. The scandals have implications far beyond U.S. borders, as other countries have emulated the U.S. model of using options

to put compensation at risk. The scandal involves the falsification of the dates options were issued to provide recipients the lowest possible price and thus the largest gain. Sadly, this defeated the purpose of options—to provide incentives for employees to contribute to the growth of their companies through rising stock prices.

The scandal is very ironic in that stock options were viewed in the 1980s as a means to reform executive pay abuses. Options were viewed by reformers as a true pay-for-performance mechanism and a major improvement over large bonuses awarded regardless of company performance. Executives and senior managers would prosper only if their company's stock value increased. Since options could only be exercised after extended periods, they would provide loyalty incentives as well.

The problem was that the options process could be easily perverted from the original intent to provide incentives for improved company performance. Until the enactment of the Sarbanes-Oxley Act, companies could declare options weeks or even months after they were granted. Under the new regulations, options have to be declared within two days. There is little evidence that option abuses have occurred after 2002, when the new regulations were imposed.

Before the new regulations, it was a simple matter to falsify the actual grant dates of stock options. It took skeptical mathematicians to determine that it was a statistically impossible coincidence that options seemed to be always granted on the lowest date for a given financial period. Even without the math, common sense should have warned auditors, regulators, and board members that something was simply too good to be true.

For the many U.S. critics who claim that the overregulation has hurt American competiveness, the stock option scandal could not have come at a worse time. Critics of Sarbanes-Oxley (SOX) and other related crackdowns argue that the corruption of the 1990s was the work of a few bad apples. With over 140 companies implicated to date, 60 executives who have lost their jobs, and the large number of prosecutions underway, it is hard to argue that this is an isolated incident. To make matters worse, there are indications that corporate directors are caught up in the scandals as well.[6]

The impact on the bottom lines of stock options abuse has been significant. When United Health restated earnings going back some five years, it was a $1.7 billion hit to the bottom line. Most other companies caught up in the scandals have been forced to restate earnings as well. Some have argued that this is a victimless crime. The truth is that investors were defrauded by investing in companies that intentionally overstated earnings.

Options have grown from under 25 percent of executive compensation in the early 1990s to over 50 percent in the early 2000s.[7] In a typical stock option program, the recipient is given a number of years to buy the company's stock at an exercise or strike price at which the options were granted. For example, if a recipient receives options at a $20 price and can exercise the options when the

stock is at $30, the person pockets a $10 profit. To assure loyalty, options can not typically be exercised for a period from the year they are granted.

Stock options still have their defenders, who argue that most companies have been ethical and judicious in their treatment. The high technology industry has been an especially strong defender of options. Cash-poor high-tech start-ups have relied on stock options in lieu of large salaries to foster loyalty and innovation.

Even though options have been granted since the 1920s, they reemerged in the late 1980s as a means to reform what was seen as excessive executive bonuses, especially in underperforming companies. Unfortunately, this was only treating the symptom and not the problem itself—weak and submissive boards of directors. CEOs and CFOs so dominated corporate boards that option oversight was doomed in many organizations. Corporate boards were often only a rubber stamp in the option approval process.

Options received a major boost from Congress when it passed legislation in 1993 that provided tax exemptions for stock options while restricting exemptions for other types of compensation. This led many companies to structure compensation packages to emphasize options. Congress also helped to head off SEC and audit firm reforms that would have forced companies to expense options. Boards also did their part by resisting suggestions to reduce the number of options granted to adjust for soaring stock prices.

Options also contributed to a tendency for executives to play accounting tricks or take short-term measures to drive up stock prices and with them the value of their options. Typical of this process has been the tendency to reprice options when the stock price changes. Companies have defended this practice by arguing that the lower stock prices destroy performance incentives. Of course stockholders do not get a chance to reprice their stock purchases, and critics correctly charge that repricing is a subversion of the entire option process. Over 10 percent of companies repriced options at least once in the mid 1990s, and one survey estimates that this had the effect of increasing executive pay on average of about $500,000. None of these actions were in the original intent and spirit of stock options to reward executives for contributing to increasing shareholder value.[8]

In response to the mounting U.S. scandals, the SEC issued much-needed stock option guidance in September 2006. The guidance references Accounting Principles Board Opinion No. 25, "Accounting for Stock Issued to Employees." Opinion No. 25 is guidance that many companies followed before the Financial Accounting Standards Board issued Statement No. 123, "Share-Based Payment." The SEC's letter provides several option scenarios in response to company inquiries. It includes a straightforward example of how to determine the measurement dates. Under Opinion 25 the measurement date is defined as the first date on which two facts are known: (1) the number of shares that an individual employee is entitled to receive and (2) an option or purchase price, if any. Some companies claimed that their measurement dates may appear incorrect

because option grants were delayed due to processing and board approval factors. The SEC's letter noted that a company's option policies and procedures usually define the required steps to make a grant effective. Although the guidance letter helped clear up some of the confusion, it does not have the force of law, as opinion letters are not approved by the SEC.[9]

8.4 WHY STOCK OPTIONS SHOULD BE AVOIDED

In our first book, *The Manager's Guide to Compliance* (John Wiley & Sons, 2006), we argued against stock options before the large majority of scandals became public. The events of the past year enforce this conclusion. Putting compensation at risk and tying compensation to performance are compendable, but there are many ways to do this without resorting to stock options. Compensation should be tied to factors within an employee's span of control. Stock prices wax and wane for a myriad of reasons beyond an employee's or even a senior executive's span of control. For senior executives, it may make more sense to tie compensation to improvements in long-term earnings and return on equity.

There are four good reasons to end stock options:

1. There have been too many shortsighted decisions, accounting tricks, and other manipulations designed to drive up stock prices at the expense of corporate long-term well-being. With 50 percent or so of executive compensation tied to options, this should come as no surprise.
2. There are better ways to compensate employees, managers, and executives for performance. They should be tied to the company's long-term strategic goals and to factors over which the recipient has some influence.
3. The current wave of scandals will take years to prosecute and litigate, leaving a bad taste in investors' mouths. Shareholders will reward corporate boards that take a proactive approach by making a clean break with options.
4. The United States is a role model for other countries. China, for one, is very interested in stock options and doomed to relive U.S. history, given its current state of corporate governance.

8.5 SUGGESTIONS IN MANAGING OPTIONS FOR THOSE WHO MUST RETAIN THEM

For those who must retain stock options, it is essential to obtain expert advice, follow a strict regime that is well documented and understood at the board and management levels, and provide complete transparency. Below is a list of recommendations in no particular order of importance that may guide organizations that can not give up the options habit.

- Clearly identify the lines of responsibility for all those involved in equity compensation. This may include the board of directors; the board's compensation committee; sub-committees of the board such as a stock option

committee; such internal personnel as human capital, finance, legal, corporate communications/investor relations; outside auditors; outside legal counsel; and third-party service providers such as stock option plan administrators; and consultants in compensation.

- Designate an internal owner and champion with overall responsibility for overseeing the end-to-end compensation process. This person needs to have easy and rapid access to appropriate members of the board and the compensation committee.
- Develop clear timelines for all related administrative functions, processes, procedures, and communications for all the parties involved.
- Incorporate compensation procedures into the company's general disclosure controls and procedures that will be transparent and fully auditable. It may be wise to ask both internal and external auditors to review and approve any changes in these procedures. These procedures should include articulating the role equity grants play in the organization's employee compensation philosophy.
- Follow practices and procedures that assure consistent and transparent actions in determining the fair market value of stock option awards.
- Develop the appropriate processes and procedures for securing the written approvals of all members of compensation and stock option committees. It is vital that there is a consensus.
- Consolidate and standardize company award grants into a smaller number of consistent, pre-scheduled grant dates, such as making new hire award grants on a set date or day each month, and making yearly award grants for all employees at the same time each year. Conversely, create a higher level of review for all special award grants.
- Strictly adhere to the organization's board charters, employment agreements, stock plans, procedural manuals, and contracts with third-party service providers. Verify the consistency between these enabling documents and communications made to shareholders about equity compensation plans and practices.
- Carefully review the process by which authority is delegated to compensation committees or to lower-level administrative committees.
- Stay abreast of share-number limitations specified in or with respect to stock plans. This includes the volume of shares reserved and available for issuance under a given plan, the volume of shares that are authorized to be reserved for issuance, or the share volume maximums that may be granted to individual employees during a given period.
- Review disclosures in the company's SEC filings or other public statements for completeness and accuracy.
- Understand and prepare for the need for grant representations by an organization's director and officer insurance carrier. In addition, legal counsel

should be involved early in the process of responding to such requests or questionnaires.

- Maintain good communication and coordination with the organization's accountants. This is especially important for special or off-cycle award grants.
- Become familiar with and follow the procedures of the organization's stock plans, board and committee charters, employment agreements, procedural manuals, and contracts with third-party service providers; and ensure consistency between these documents and communications made to shareholders about equity compensation plans and practices.
- Review disclosures in the company's SEC filings or other public statements for completeness, consistency, and accuracy. As of December 15, 2006, an organization's proxy statements have to provide extensive disclosure about option grant practices, including practices relating to spring loading and bullet dodging grants.
- Keep current on the changes in technical requirements over equity compensation. This includes disclosure, tax, and accounting rules. The SEC's new executive compensation disclosure rules and FAS 132 R are good examples of the difficulty in hitting a moving target.
- Pay special attention to authority delegated to compensation committees or to lower-level administrative committees. The measurement of fair market value of the company stock should be made as of the actual grant date by the lower-level administrative committee and not by the date the compensation committee delegates authority.
- Pay particular attention to share-number limitations specified in stock plans. This is the maximum numbers of shares that may be granted to individual employees during certain periods or the total number of shares available for issuance under a plan.
- The overall philosophy of the organization should include a determination as to whether equity grants are to be a regular part of the compensation of all salaried employees or only of higher level executives and senior managers.

8.6 HOW THE UNITED STATES GOT INTO SUCH A MESS

In an October 2006 speech, Linda Chatman Thomsen, the SEC's Director, Division of Enforcement, outlined how the US got into such a mess over stock options.

"*First*, beware the morphing monster—and its unintended consequences. Tools devised for one purpose can have dramatic unintended consequences when employed for different purposes in a different legal and tax environment. We've seen this happen over and over again. One example is the "Special Purpose Entity" or "SPE," which was designed as a special form of off-balance sheet accounting

originally used in the aircraft industry. But SPEs migrated into other industries and morphed into a monster that was used extensively by the likes of Enron in perpetrating financial frauds . . . Similarly, stock options were initially developed in the 1980s as an anti-takeover device, but because of unrelated changes in the tax and accounting rules, they morphed into a means of providing non-salary performance-based compensation, which was not their original purpose. And as we have seen, to the extent that stock option grants were viewed in the 1990s as a means of better aligning the interests of management and corporate shareholders by linking executive compensation to performance, they had yet another set of unintended consequences."

"*Second*, your mother was right—just because your best friend jumps off a bridge doesn't mean you should too. Clearly, a lot of companies were involved in options backdating, but that doesn't excuse the fundamentally fraudulent nature of the scheme. If the only reason that can be offered as a justification for backdating is that "everyone else was doing it," that's a poor excuse for what amounts to unjust enrichment of a few employees at the expense of corporate shareholders."

"*Third*, the simplest and most obvious lesson, you can't have your cake and eat it too. A stock option can be granted either in the money or at the money, but not both. You can take your pick, but you have to accept the consequences of your choice."

"*Fourth*, process can be your friend. This is a variant of the "sunscreen and dental floss" rule. You see, both sunscreen and dental floss can have tremendous benefits, but only if you use them every single day. In the same way, if a company devises a specific lawful process for granting employee stock options and always follows it, there should be no problem explaining how, when and at what price any particular options were granted. The problems we are seeing with stock option abuses often seem to occur when a company abandons its regular process and starts to award stock options on an ad hoc basis."

"The *fifth* lesson: If you are ever in doubt about whether any particular practice is right, imagine explaining it to your family, especially your children. This "explain-it-to-your-family" exercise has two advantages. To start with, you have to simplify and distill whatever it is you're contemplating down to its essence. The very process of simplifying the concept to its essence will usually enable you to see its true strengths and weaknesses. The other advantage is that you're pitching your plan to a supportive audience, but one that will give you their real opinions. If you want a really objective view of what you're doing, try asking a teenage boy. Teenage boys will tell you, in detail, all the flaws in your plan, and, for that matter, everything else you're doing. If you want more support, you might try your spouse—well, that depends. But if you can't imagine explaining to your children or other family members why what you're contemplating is the right thing to do, then you shouldn't do it . . ."

"*Finally*, what we have learned from stock options backdating—and from every other scandal in the financial markets in recent years—is that character

matters. Corporate character matters—and employees take their cues from the top. In our experience, the character of the CEO and other top officers is generally reflected in the character of the entire company. If a CEO is known for his integrity, integrity becomes the corporate norm. If, on the other hand, a company's top executives are more interested in personal enrichment at the expense of the shareholders, our backdating investigations demonstrate yet again that other employees will follow suit."[10]

Notes

1. Weil, Gotshal, and Manges, LLP, "Option and Other Equity Grant Practices," Weil Corporate Governance Briefing, February 22, 2007.
2. Ibid.
3. Ibid.
4. Ibid.
5. Wikipedia, "Employee Stock Option," http://en.wikipedia.org/wiki/Employee_stock_option.
6. Alan Murry, "Will Backdating Scandal Thwart Effort to Roll Back Reforms?" *Wall Street Journal*, December 20, 2006, A2.
7. Mark Maremont and Charles Forelle, "Open Spigot—Bosses' Pay: How Stock Options Became Part of the Problem; Once Seen as a Reform, They Grew into Font of Riches and System to Be Gamed," *Wall Street Journal*, December 27, 2006, A1.
8. Ibid.
9. Helen Shaw, "SEC Issues Option Accounting Guidance: New Guidance from the Chief Accountant Tells Companies How to Respond to Various Outcomes of Internal Investigations into Backdating and Other Stock Option Granting Problems," CFO.com, September 19, 2006.
10. Linda Chatman Thomsen, SEC Director, Division of Enforcement, "Speech By SEC Staff: Option Backdating—The Enforcement Perceptive," Washington, D.C., October 30, 2006.

CHAPTER 9

FRAUD AND CORRUPTION

Hrishikesh D. Vinod

The topic discussed in this chapter is rather vast in its scope and impossible to cover within the confines of a single chapter. For brevity, I will focus on topics with which I am most familiar as evidenced by my own publications and refer the reader to those sources for additional information, detailed references, and background discussion. The chapter is divided into seven sections with descriptive self-explanatory titles.

9.1 WHAT ARE FRAUD AND CORRUPTION? HISTORICAL BACKGROUND FROM ETHICS

Fraud and corruption have many facets, including cultural, legal, socioeconomic, and ethical aspects. Fraud is defined as deliberate deception designed for gain by hurting another person's interests. Corruption is defined as abuse of a position of trust for dishonest gain, such as taking a bribe. An economist's or business manager's materialistic definitions of fraud and corruption refer to all unethical behavior, which can be illustrated by business deception and bribery. Ethics may

appear to belong to the realm of morality and theology, but actually does have considerable role in our context. Analytical methods used by economists do heed ethical considerations, often under the headings of income distribution, economic justice, and regulation.

Ancient humans instinctively thought of fraud and corruption as immoral and therefore inconsistent with material and spiritual well-being of citizens. Aristotle asked in Chapter 4 of *Politics:* "What sort of wealth-getting activity is necessary and honorable for humans to undertake?" He was perhaps the first to study the practical question of human relationships in the context of material environment. He also said in Chapter 8: "The amount of property which is needed for a good life is not unlimited."

Ancient philosophers often blamed crass materialism for fraud and corruption and therefore took an antiwealth stance to discourage cheating and a tendency to achieve material wealth by hook or by crook. For example, spiritual well-being was emphasized by Stoic philosophers like Marcus Aurelius, who appealed to achieving true happiness by submission to destiny, not by deception. Similarly, Arab-Islamic scholars were not antiwealth, but did believe in the role of fate or kismet. The Biblical story that it is easier for a camel to pass through the eye of a needle than for a rich man to get into heaven is quite explicit. An open disdain for wealth may be read in some Jewish, Hindu, and Chinese philosophy. Major religions preach against fraud and corruption by pointing to the will of God and to natural law, and rarely through rational arguments.

During the Italian renaissance, Thomas Aquinas asked a number of practical questions in the world of commerce and morality. He wondered whether it is ethical and legal to sell an item for more than it is worth, and explicitly considers moral obligations of sellers and buyers. It is possible to read his work *Summa Theologica* as a guidebook for commercial behavior. He considered failing to reveal information about an item's defect as cheating. In his time most people lived in a subsistence economy; when markets were not well established, there was no practical way to determine the fair worth of anything except by tradition. Hence it was perhaps appropriate for Aquinas to insist on buying and selling at the true intrinsic worth of items. He was concerned with living the good life and being a good citizen. His philosophy contains the rudiments of the following purely rational argument against fraud and corruption: If a great many citizens deceive each other and if government officials are corrupt, a good life through commerce is impossible.

Clearly, honestly earned wealth must be distinguished from ill-gotten riches, and a government is needed to punish the cheaters and bribe takers. Aristotle was the first to make this distinction explicit. As capitalism developed, honestly earned wealth began to be admired. Besides Aquinas, John Calvin was responsible for the development of the Protestant ethic, which thought of wealth acquisition as virtuous, not sinful; encouraged prudent use of wealth; and indirectly laid the foundation for capital accumulation made possible by the industrial revolution.

Thomas Munn was an East India Company officer. His essay "England's Treasure by Foreign Trade" argued that wealth accumulation, which made businesspeople rich, also contributed to the economic and political strength of England. His was an influential articulation of the Protestant ethic. Munn also supported colonialism and expected the British government to support the commercial activities of the likes of the East India Company. He was also a mercantilist supporting globalization of his era, and was concerned with trade balances, exchange rates, and capital movements. Mercantilists were focused on enriching the king and strengthening national power, rather than raising the living standards of the common folk. Mercantilists thought of trade as a zero-sum game in which one country gained what the other lost. Their gains and losses were measured by gold and power, while morality was unimportant.

Adam Smith's celebrated work *The Wealth of Nations* attacked mercantilism and was preceded by *The Theory of Moral Sentiments*. It is interesting that Smith emphasized division of labor and human capital, not gold. Smith strongly criticized greed and callousness of capitalists and argued for the importance of ethics for a prosperous society.

Jeremy Bentham focused on self-interest as the main motivation and did not want to wait for Smith's "invisible hand" to right the existing social inequalities. He proposed legislation changing the Poor Law and advocated education for the working class. John Stuart Mill argued that human motivation includes sympathy and benevolence. Mill took a more nuanced modern approach to morality and laissez-faire economics. He understood the so-called problem of the commons, or the unique nature of public goods, which are best provided by the government.

There are two views of human nature in a business context. In the liberal camp we have Aristotle, John Locke, Adam Smith, Jeremy Bentham, and John Stuart Mill, among others, who saw humans as good and rational. This view supports limited government and limited interference with individual choices. By contrast, classical conservatives included Augustine, Aquinas, Hobbes, and Machiavelli, who saw humans as greedy, irrational, even bestial, and supported a strong central governing authority. Since excess regulation can kill entrepreneurial spirit, public opinion and policy generally swing between these two views with distinct practical implications for control of fraud and corruption.

9.2 CONSEQUENCES OF FRAUD AND CORRUPTION FOR AN INDIVIDUAL, BUSINESS, AND COMMUNITY

The consequences of fraud and corruption for an *individual* perpetrator obviously depend on whether he or she is caught, which in turn depends on the level of enforcement of antideception and antibribery laws, and on the role of the media in exposing and shaming the miscreants. The consequences for a small business perpetrator are mostly similar. By contrast, fraud and corruption in larger businesses have important consequences for the following stakeholders: shareholders, customers, suppliers, employees, managers, and local governments. This

section argues that due to these undesirable consequences, fraud and corruption need to be minimized with eternal vigilance, even if they cannot be eliminated altogether.

Vinod (1999) is one of the first empirical papers to study the consequences of corruption on the domestic economies of various countries using data on 16 socioeconomic and political variables. In this cross-sectional study Vinod shows the relevance of red tape and efficiency of judiciary to explain the corruption perception index (CPI) of a country. Transparency International regularly publishes the CPI, using a carefully designed survey of businesspeople, professional risk analysts, and the public. Vinod relies on subset regression methods using Mallows' Cp and Akaike information criteria (AIC) and finds that better schooling and reduced income inequality can help reduce corruption. He also shows that corruption is similar to an uncertain tax and estimates that a dollar's worth of corruption imposes $1.67 worth of a burden on the domestic economy.

The consequences of corruption on the international economy are also severe, as explained in Vinod (2003) and illustrated by the 1997 Asian contagion and banking distress, popularly blamed on crony capitalism in those countries. The consequences are worse in countries where the financial sector is inefficient. A well-developed financial derivatives market is helpful in managing different risks, including credit risk, default risk, risk of fraud, and so on. Thin or inefficient derivatives markets in the absence of scale economies can exacerbate any contagion when international investors rebalance their portfolios across countries. Financial institutions themselves are hurt by contagion in several ways, including loss of physical assets, loss of goodwill, and loss of stock value due to manipulation and fraud. Moreover, corruption erodes the trust in the local financial institutions. Sometimes rating agencies cause the proliferation of herd behavior or self-fulfilling prophecies.

International trade is known to be subject to a refusal of investors to diversify their portfolios across countries, or home bias. When developing countries are included in the picture, instead of home bias one observes flight of capital away from poor and corrupt countries. Hence policy makers impose capital controls to prevent the much-needed domestic capital from leaving the country. However, capital controls themselves often further promote monopolies and corruption. Using the International Monetary Fund (IMF) annual report, Vinod (2003) creates an "index of capital controls" and shows that capital flight controls themselves might discourage foreign direct investment (FDI). Data show that investors more heavily weight potential costs of corruption, especially if they use value at risk (VaR) analytical methods, popular for choosing among portfolios. This is not surprising, since VaR means a study of worst-case scenarios.

Vinod (2003) verifies that corruption does increase the cost of capital, by using data from PricewaterhouseCoopers, which reports percentage penalty

in terms of capital due to lack of transparency and corruption in 34 countries. Vinod (2003) reports that following correlation coefficients are statistically significant: (1) between the corruption perception index (CPI) and the FDI/GDP ratio (showing that FDI goes to countries with less corruption); (2) between CPI and the trade/GDP ratio (showing that with trade comes more foreign competition and less corruption); (3) between CPI and the capital flow control index (suggesting that controls themselves encourage corruption); and (4) between CPI and the cost of capital percentage penalty. Data show that corrupt countries pay a penalty when they borrow in international financial markets and that the penalty decreases as the corruption in the country decreases.

In short, the cost of investing in a corruption-ridden country is very high, thus leading to a reduction in FDI. The greater uncertainty caused by corruption means a larger risk premium. In conclusion, in both open and closed economies, corruption can have several strong detrimental effects.

9.3 PRINCIPAL-AGENT PROBLEM WITH PRACTICES AND PROCEDURES FOR MANAGING FRAUD AND CORRUPTION

The principal-agent problem is a name given by economists to a common problem in almost all employer-employee relationships, where the employer has incomplete information about the motives and activities of the employee. See Sappington (1991) and Prendergast (1999) for surveys of the literature. The employees of governmental bodies or businesses are often tempted to achieve personal gains at the cost of the employer, such as by taking bribes, especially if they can get away with it and all records can be erased. It is very difficult to police such corruption, since the private gain may include nonmeasurable things such as sexual favors or donations to favorite charities or political parties, and the private gains might be granted to third parties.

Most tools commonly used for aligning the interests of the employee (or agent) with those of the employer (or principal) have the following themes:

- Make employee compensation directly proportional to the employer's gain. This includes efficiency or piece wages, commissions, and profit sharing. A relatively recent example is the granting of stock options or other deferred compensation such that it is positive only of the stock price goes up. Of course we must guard against fraud (backdating) and misuse of these schemes (manipulation of quarterly earnings reports by hiding losses in offshore and/or off-balance-sheet entities). All these compensation schemes can fail if employer's profits depend on employee team effort rather than individual hard work.
- Threaten the employee with sanctions such as the loss of the job, a deposit, a bond, a cut in compensation in the form of a significant fine, or public humiliation.
- Use special rewards and prizes (e.g., employee of the month).

- Use surveillance cameras, anonymous reports by independent observers, private investigators, and whistle-blowers to expose miscreants and reward team players.
- Since it might take a thief to catch a thief, peer reviews can be useful.
- Use profiling of employees and make intensity of monitoring proportional to past transgressions, however minor. This can include providing networking opportunities for employees who benefit the employer.

We conclude this section by noting that the fight against fraud and corruption is not hopeless.

9.4 BEST PRACTICE GUIDELINES FOR DETECTION METHODS, INCLUDING CHECKING OF BACKGROUND AND REFERENCES

Honest and moral behavior can often be traced to upbringing at home. Background checks on individuals are often valuable tools for ensuring that convicted perpetrators are not inadvertently hired in sensitive positions. The managers should treat these checking activities with the seriousness they deserve and bring modern science to bear on these tasks. Evidence of a past criminal record or drug use often flags problematic employees who should not do sensitive jobs. Of course, the employer has to be aware of scams and be sure to check the background checkers themselves. The reference names given by employees should be independent, and a lack of good references can be indicative of potential problems. Mental health, marital relations, genetics, credit reports, Internet searches, and travel histories can also be relevant. Specialized forensic accountants are sometimes used for preventing fraud and corruption. Great care is needed in using these investigative tools and while handling personal data, since it is immoral (and generally illegal) to invade the privacy of employees.

9.5 DATA MINING FOR DETECTION OF FRAUD AND CORRUPTION

A large corporation routinely collects a great many measurements, which inevitably interact with employee activities. There are data on all kinds of expenses, telephone usage, visitors, energy use, travel, and the like. Most examples of fraud and corruption can manifest themselves in these routine measurements in subtle ways. Fraudsters often have measured values that do not fit a common pattern, trend, known evolution, or known long-memory stochastic process. In traditional statistics these measurements are called outliers and their detection was originally intended for the purpose of cleaning of data. Statistical outlier detection methods were developed long ago in the context of quality assurance using the fact that normal distribution varies within three standard deviations of the mean, but have been extended to far more general nonnormal, nonlinear models with the advent of computers.

A fancier name for outlier detection is computer-intensive knowledge discovery and data mining (KDD). It has become a field of study widely used in health

care, retail, credit card services, telecommunications (phone card fraud), and so on. The basic idea is to use historical data to build behavior models for detecting unusual activities flagging potential fraud and corruption. Here are some examples.

- The insurance industry uses KDD to detect those who stage automobile accidents to collect insurance, and to catch professional patients and dishonest doctors.
- The U.S. Treasury's Financial Crimes Enforcement Network uses KDD to detect money laundering.
- British Telecom uses KDD for studying the destination, duration, and timing of phone calls to apprehend fraudulent callers.
- KDD helps the retail sector reduce large losses due to employee theft and other abuses.

All KDD involves a form of machine learning of human behavior, which in turn requires careful data selection, cleaning, reduction, and transformation to reduce its dimensionality. Various multivariate statistical tools, including cluster analysis, principal component, canonical correlation, discriminant analysis (Vinod and Ullah1981, ch. 12), are used in data mining to evaluate joint multivariate patterns with a view to finding outlier patterns for further investigation. Decision trees and neural networks mentioned in Vinod and Reagle (2005, sec. 6.3) are also useful. There are no magic KDD tools, just painstaking application of usual tools that generalize, summarize, classify, predict, and contrast data characteristics. Vinod (1969) provides the mathematical programming model for clustering, where the basic aim is to minimize within group sum of squares (WGSS) and maximize between group sum of squares (BGSS), which is more general than hierarchical clustering models. These multivariate methods have become more practical with the availability of powerful computers.

Data mining for detection of fraud and corruption has obvious applications in detecting terrorist cells, and therefore some of the research in this area is likely to be classified. There are a number of public domains (e.g., www.r-project.org) and other software products for accomplishing what is suggested here, and the possibilities keep expanding as experience is gained.

9.6 CORPORATE GOVERNANCE, COMPLIANCE ISSUES, AND KNOWING YOUR EMPLOYEES AND CLIENTS

Corporate governance mostly refers to government regulation controlling self-governance of corporations as business entities. In this section, let us focus on organizational structures preventing ethical lapses before they occur. Although the interest of shareholders (owners) must remain supreme in a capitalist system, the *long-term* interest of those owners and society lies in fair treatment of all stakeholders: owners, managers, employees, clients, governmental entities, and the general public. A successful business is impossible in the long run without trust among the stakeholders built on a foundation of fair play.

Efficient corporate governance requires appropriate record keeping, clear assignment of responsibility, and suitable public disclosure (perhaps on the Internet) of past actions and future plans. Although any business will have some secrets it would like to keep from its competitors, a good corporate governance regime must strike a proper balance between secrecy and transparency. Similarly, a balance is needed between delegation and concentration of authority, along with proper checks and balances on almost all exercises of discretion and power.

The following anecdote illustrates the necessity of government regulation and the difficulty of enforcing morality. A city boy, Kenny, moved to the country and bought a donkey from an old farmer for $100. The farmer agreed to deliver the donkey the next day. However, the next day the farmer drove up and announced, "Sorry, son, but I have some bad news! The donkey died." Kenny replied, "Well then, just give me my money back." The farmer said, "Can't do that, since I've already spent it all." Kenny answered, "Okay then, at least give me the donkey." The farmer asked, "What're you gonna do with him?" Kenny said, "I'm going to raffle him off." The farmer exclaimed, "You can't raffle off a dead donkey!" Kenny said, "Sure I can. Watch me. I just won't tell anybody he is dead." A month later the farmer met up with Kenny and asked, "What happened with that dead donkey?" Kenny answered, "I raffled him off. I sold 500 tickets at two dollars a piece and made a profit of $898." The farmer asked, "Didn't anyone complain?" Kenny replied, "Just the guy who won. So I gave him his two dollars back." The anecdote suggests fraudsters can come up with new schemes and it can be difficult for regulators to anticipate and stay ahead of them.

Prevention of fraud and corruption in all corporations is greatly helped by efficient governance of financial institutions. Many of the corporate scandals in recent years have resulted in large fines (exceeding a billion dollars) being paid by financial institutions, because they were complicit in the fraud. After all, banks do know a great deal about the corporate borrowers. We should blame the 1999 Gramm-Leach-Bliley Act, which sanctioned financial conglomerates, while doing little to curb newly created conflicts of interest. A banker is also a bond trader, a foreign exchange dealer, an investment broker, an insurance agent . . .; the list keeps growing as the boundaries blur and conflicts of interest proliferate.

Money center banks and large brokerage houses are often lenders to businesses in their role as investment bankers. They are also advisors to individual savers who want to lend. This means they are representing the interests of buyers and sellers of investment funds. Vinod (2004) argues that, just like the same law firm cannot honestly represent both the prosecution and the defense in a lawsuit, it is impossible for this fundamental conflict of interest to disappear by any artificial tools, such as the so-called Chinese wall forbidding communication. With the availability of fast money transfers, the need for vigilant supervision of banks is great. There are glaring examples of bank failures due to failure of supervision. In 1995 a 233-year-old bank called Barings Bank collapsed when one trader (Nicholas W. Leeson) notched up losses of $1.40 billion in his derivatives

trading. A study by the IMF put the taxpayers' total bill for resolving banking crises in emerging countries since 1980 at $250 billion. America's savings and loan troubles cost around 2 percent of GDP. The reason for a specific focus on the banking sector is that there is a paradox when private bank failure leads to public rescue with taxpayer funds.

The Enron example illustrates several failures of corporate governance discussed in Vinod (2002), who also called for expensing of stock options to prevent managerial abuses. The Financial Accounting Standards Board (FASB) has recently adopted such expensing, which was opposed by the same companies that are found accused of fraudulent backdating (*Wall Street Journal*, August 14, 2006, C1). However, the Sarbanes-Oxley Act (SOX) of 2002 is a good example of a thoughtful response, which deserves to be copied in other countries. Tarantino (2006) discusses SOX in great detail. The United States has the same excesses as any corrupt country, but also has the alphabet soup (SEC, Federal Reserve, FAA, FDA, FBI, EPA, IRS, INS, etc.) of vigilant agencies run by mostly uncorrupt bureaucrats who consistently expose, punish, regulate, and ultimately reform those excesses. America's moral authority to lead the capitalist world derives from the efficiency of these U.S. government agencies and bureaucrats.

Unfortunately, the implementation of SOX did not include sufficient practical compliance guidelines for small businesses. In fact, these uncorrupt bureaucrats should have allowed posting on the Internet of answers to simple compliance questions. Clearly, SOX is evolving and simple procedures should be forthcoming so that a well-governed small corporation can obtain a compliance certificate without much cost. Instead, the accounting profession has abused SOX to charge large fees, burdening the small and medium-sized businesses. It is interesting that closely held companies are embracing SOX's internal controls due to pressure from customers, lenders, directors, and owners wishing to take the company public in the future (*Wall Street Journal*, August 14, 2006, B3).

A rather comical list of the effects of executive self-dealing is instructive (Paul Krugman, *New York Times*, June 21 2002). Imagine that you manage an unprofitable ice cream parlor. How can you get rich? Here are strategies for executive self-dealing.

- *Enron strategy.* Sign contracts to provide customers with an ice cream cone a day for the next 30 years. Deliberately underestimate the cost, and book all the projected profits on future ice cream sales as this year's bottom line. Your business appears highly profitable and the stock price goes up!
- *Dynegy strategy.* Convince investors that you will be profitable in the future. Enter into a quiet agreement with another ice cream parlor in which each will pretend to buy hundreds of cones daily in order to appear to be a big player in a coming business, and sell shares at inflated prices.
- *Adelphia strategy.* Sign contracts with customers, and get investors to focus on the volume of contracts rather than their profitability. Instead

of imaginary trades, invent imaginary customers. Stock analysts give you high marks, and you can sell shares at inflated prices.

- *WorldCom strategy.* Make real costs disappear by pretending that operating expenses—cream, sugar, chocolate syrup—are part of the purchase price of a new refrigerator, so you appear to borrow only for new equipment. You can then sell shares at inflated prices.
- *Fictitious asset sale (Enron, Harken Energy) strategy.* Sell your ice cream delivery van to XYZ Inc. for an outlandish price to claim capital gain as profit. Actually you own XYZ secretly anyway. In all this, top managers benefit through stock options, Adelphia-style personal loans, and other devices.

We conclude the section on corporate governance in the United States by urging a ban on self-dealing and stricter control of numerous other abuses by top executives. We need healthy skepticism, as well as sharp eyes, ears, and nose by the board of directors, supported by independent no-nonsense auditors (inspectors general) well versed in criminology in addition to law and accounting.

9.7 ENFORCEMENT, INCENTIVE SCHEMES, AND MARKET SOLUTIONS PREVENTING FRAUD AND CORRUPTION

Prevention of fraud and corruption is far better than enforcement through punishment. Hence we now discuss some tools for preventing corrupt behavior by using standard administrative and regulatory mechanisms to discourage persons with discretionary power from misusing that power for personal gain. First, disclosure of personal assets and liabilities of public officials and their close relatives means that they cannot hide any significant bribes received without being noticed. In some cases local officials are too beholden to the locally powerful individuals and entities. Then, an international monitoring authority might be needed to enforce transparency of public sector contracts.

For example, a group of countries can sign long-term integrity pacts, with suitable sharing of information and coordination of investigations into fraudulent dealings. Another preventive tool is to simplify procurements by reducing procedural complexities and discretion. Corruption can be in the form of concealed payments and illegal transfers of valuable public assets to "sweethearts" of officials. It is important to remove potential incentives for exchanging favors and all quid pro quo payments. We have to prohibit corrupt officials from taking public or third-party time and resources hostage.

Market solutions to prevent fraud and corruption include liberalization, expanded foreign trade, privatization, and more generally providing customers with wider choices and fuller information. Liberalization means creating a competitive, transparent, and level playing field for all competitors. Market reforms can be genuine only if government refrains from directly owning commercial enterprises and managing markets. Moreover, the reforms need to be coupled with

sound rules of the game, administered by impartial regulators in an environment free of outside (political) interference.

As a practical matter, public servants should know their rights (presumption of innocence, due process, etc.) and obligations in the context of such wrongdoing. The officials need clear guidelines regarding their normal interactions with their friends, relatives, general public, businesspeople, and political leaders. It is important that management policies, procedures, and practices promote ethical conduct and that there are good role models. When unethical conduct is uncovered, the person responsible should be held accountable for the lapse, while the punishment process should be transparent and open to scrutiny. Prompt and appropriately transparent sanctions should be imposed, and current procedures should be improved whenever possible to discourage similar misconduct in the future.

This chapter began with a historical philosophical review of the role of ethics in business transactions. We defined fraud and corruption and indicated its consequences in both domestic and international arenas. Despite unavoidability of the principal-agent problem, we argued that the situation is not hopeless by listing best practice guidelines, use of data mining statistical tools, and corporate governance regimes. We also discussed prevention and enforcement tools, including some involving market incentives.

References

Prendergast, C. 1999. The provision of incentives in firms. *Journal of Economic Literature* 37 (March): 7–63.

Sappington, D. E. M. 1991. Incentives in principal-agent relationships. *Journal of Economic Perspectives* 5 (2) (Spring): 45–66.

Tarantino, A. 2006. *The manager's guide to compliance*. Hoboken, NJ: John Wiley & Sons.

Vinod, H. D. 1969. Integer programming and the theory of grouping. *Journal of the American Statistical Association* 64 (June): 506–519.

Vinod, H. D. 1999. Statistical analysis of corruption data and using the Internet to reduce corruption. *Journal of Asian Economics* 10: 591–603.

Vinod, H. D. 2002. Winners and losers in multiple failures at Enron and some policy changes. Social Science Research Network (SSRN). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=300542.

Vinod, H. D. 2003. Open economy and financial burden of corruption: Theory and application to Asia. *Journal of Asian Economics* 13: 873–890.

Vinod, H. D. 2004. Conflict of interest economics and investment analyst biases. *Brooklyn Law Review* 70 (1) (Fall): 53–88.

Vinod, H. D., and D. Reagle. 2005. *Preparing for the worst: Incorporating downside risk in stock market investments*. Hoboken, NJ: John Wiley & Sons.

Vinod, H. D. and A. Ullah. 1981. *Recent advances in regression methods*. New York: Marcel Dekker.

CHAPTER 10

WHY FIGHTING CORRUPTION REMAINS A LOSING BATTLE

Anwar Shah

10.1 INTRODUCTION: THE FIGHT AGAINST CORRUPTION REQUIRES A DEEPER UNDERSTANDING OF THE UNDERLYING MALAISE

Statistics on corruption are often questionable, but available data suggest that it accounts for a significant proportion of economic activity worldwide.[1] In Kenya, "questionable" public expenditures noted by the controller and auditor general in 1997 amounted to 7.6 percent of gross domestic product (GDP). In Latvia, a recent World Bank survey found that more than 40 percent of households and enterprises agreed that "corruption is a natural part of our lives and helps solve many problems." In Tanzania, service delivery survey data suggests that bribes paid to officials in the police, courts, tax services, and land offices amounted to 62 percent of official public expenditures in these areas. In the Philippines, the Commission on Audit estimates that $4 billion is diverted annually because of public sector corruption (see Anwar Shah and Mark Schacter 2004).

Moreover, a study by Tomaszewska and Shah (2002) of the ramifications of corruption for service delivery concludes that an improvement of one standard deviation in the International Country Risk Guide corruption index leads to a

29 percent decrease in infant mortality rates, a 52 percent increase in satisfaction among recipients of public health care, and a 30 to 60 percent increase in public satisfaction stemming from improved road conditions. Studies also show that corruption hurts growth, impairs capital accumulation, reduces the effectiveness of development aid, and increases income inequality and poverty (World Bank 2004).

Not surprisingly, therefore, there has been a growing global movement to condemn corrupt practices, in fact resulting in the removal of some country leaders. In addition, many governments and development agencies have devoted substantial resources and energy to fighting corruption in recent years. Even so, it is not yet clear that the incidence of corruption has declined perceptibly, especially in highly corrupt countries. This chapter argues that the lack of significant progress can be attributed to the fact that many programs are simply folk remedies or one-size-fits-all approaches and offer little chance of success. For programs to work, they must identify the type of corruption they are targeting and tackle the underlying, country-specific causes, or drivers, of dysfunctional governance. This chapter examines the conceptual and empirical basis of these concerns. Section 10.2 defines corruption and governance and discusses the importance of current concerns about corruption.[2] Section 10.3 provides analytical and empirical perspectives on corruption. The final section presents some conclusions.

10.2 CORRUPTION AND GOVERNANCE: FUNDAMENTAL CONCEPTS AND CONCERNS

Corruption is defined as exercise of official powers against public interest or the abuse of public office for private gains. Public sector corruption is a symptom of failed governance. Here, we define *governance* as the norms, traditions, and institutions by which power and authority in a country are exercised—including the institutions of participation and accountability in governance, the mechanisms of citizens' voice and exit, and the norms and networks of civic engagement; the constitutional-legal framework and the nature of accountability relationships among citizens and governments; the process by which governments are selected, monitored, held accountable, and renewed or replaced; and the legitimacy, credibility, and efficacy of the institutions that govern political, economic, cultural, and social interactions among citizens themselves and their governments.

Concern about corruption—the abuse of public office for private gain—is as old as the history of government. In 350 B.C.E., Aristotle suggested in *The Politics* that "to protect the treasury from being defrauded, let all money be issued openly in front of the whole city, and let copies of the accounts be deposited in various wards." In recent years, concerns about corruption have mounted in tandem with growing evidence of its detrimental impact on development (see World Bank 2004). Corruption is shown to adversely affect GDP growth (Mauro 1995; Abed and Davoodi 2000). Corruption has been shown to lower the quality of education (Gupta, Davoodi, and Tiongson 2000), public infrastructure (Tanzi

and Davoodi 1997), and health services (Tomaszewska and Shah 2000; Triesman 2000), and to adversely affect capital accumulation. It reduces the effectiveness of development aid and increases income inequality and poverty (Gupta, Davoodi, and Alonso-Terme 1998). Bribery, often the most visible manifestation of public sector corruption, harms the reputation of and erodes trust in the state. As well, poor governance and corruption have made it more difficult for the poor and other disadvantaged groups, such as women and minorities, to obtain public services. Macroeconomic stability may also suffer when, for example, the allocation of debt guarantees based on cronyism, or fraud in financial institutions, leads to a loss of confidence by savers, investors, and foreign exchange markets. For example, the Bank of Credit and Commerce International (BCCI) scandal, uncovered in 1991, led to the financial ruin of Gabon's pension system, and the corrupt practices at Mehran Bank in the Sindh Province of Pakistan in the mid-1990s led to a loss of confidence in the national banking system in Pakistan.

(a) THE MANY FORMS OF CORRUPTION. Corruption is not manifested in one single form; indeed, it typically takes at least four broad forms.

1. *Petty, administrative, or bureaucratic corruption.* Many corrupt acts are isolated transactions by individual public officials who abuse their office, for example, by demanding bribes and kickbacks, diverting public funds, or awarding favors in return for personal considerations. Such acts are often referred to as petty corruption even though, in the aggregate, a substantial amount of public resources may be involved.
2. *Grand corruption.* The theft or misuse of vast amounts of public resources by state officials—usually members of, or associated with, the political or administrative elite—constitutes grand corruption.
3. *State or regulatory capture and influence peddling.* Collusion by private actors with public officials or politicians for their mutual, private benefit is referred to as state capture. That is, the private sector captures the state legislative, executive, and judicial apparatus for its own purposes. State capture coexists with the conventional (and opposite) view of corruption, in which public officials extort or otherwise exploit the private sector for private ends.
4. *Patronage/paternalism/clientelism and being a team player.* Using one's official position to provide assistance to clients having the same geographic, ethnic, and cultural origin so that they receive preferential treatment in their dealings with the public sector, including public sector employment is another form of corruption, as is providing the same assistance on a quid pro quo basis to colleagues belonging to an informal network of friends and allies.

It is also known that corruption is country-specific; thus, anticorruption approaches that apply common policies and tools (that is, one-size-fits-all

approaches) to countries in which acts of corruption and the quality of governance vary widely are likely to fail. One needs to understand the local circumstances that encourage or permit public and private actors to be corrupt.

Finally, we know that if corruption is about governance and governance is about the exercise of state power, then efforts to combat corruption demand strong local leadership and ownership if they are to be successful and sustainable.

10.3 WHAT DRIVES CORRUPTION?

Public sector corruption, as a symptom of failed governance, depends on multitude of factors, such as the quality of public sector management, the nature of accountability relations between the government and citizens, the legal framework, and the degree to which public sector processes are accompanied by transparency and dissemination of information. Efforts to address corruption that fail to adequately account for these underlying drivers are unlikely to generate profound and sustainable results. To understand these drivers, a conceptual and empirical perspective is needed to grasp why corruption persists and what can be a useful antidote. At the conceptual level, a number of interesting ideas have been put forward.[3] These ideas can be broadly grouped together in three categories: (1) principal-agent or agency models, (2) new public management (NPM) perspectives, and (3) neo-institutional economics frameworks.

(a) CONCEPTUAL PERSPECTIVES.

(i) Principal-Agent Models. The most widely used modeling strategy is the principal-agent or agency model. A common thread in these models is that the government is led by a benevolent dictator, the principal, who aims to motivate government officials (agents) to act with integrity in the use of public resources (see Becker 1968; Becker and Stigler 1974; Banfield 1975; Rose-Ackerman 1975, 1978; Klitgaard 1988, 1991; Becker 1983). One such view, the so-called crime and punishment model by Gary Becker (1968), states that self-interested public officials seek out or accept bribes so long as the expected gains from corruption exceed the expected costs (detection and punishment) associated with corrupt acts. Thus, according to this view, corruption could be mitigated by (1) reducing the number of transactions over which public officials have discretion, (2) reducing the scope of gains from each transaction, (3) increasing the probability for detection, and (4) increasing the penalty for corrupt activities.

Klitgaard (1988) restates this model to emphasize the unrestrained monopoly power and discretionary authority of government officials. According to him, corruption equals monopoly plus discretion minus accountability. To curtail corruption under this framework, one has to have a rules-driven government with strong internal controls and with little discretion to public officials. This model gained wide acceptance in public policy circles and served as a foundation for empirical research and policy design to combat administrative, bureaucratic, or petty corruption. Experience in highly corrupt countries, however, contradicts the effectiveness

of such an approach, as the rules enforcers themselves add extra burden of corruption and lack of discretion is also thwarted by collusive behavior of corruptors. In fact, lack of discretion is often cited as a defense by corrupt officials who partake in corruption as part of a vertically well-knit network enjoying immunity from prosecution.

Another variant of principal-agent models integrates the role of legislators and elected officials in the analysis. In this variant, high-level government officials—represented by legislators or elected public officials—institute or manipulate existing policy and legislation in favor of particular interest groups—representing private sector interests and entities or individual units of public bureaucracy competing for higher budgets—in exchange for rents or side payments. In this framework, legislators weigh the personal monetary gains from corrupt practices and improved chances of reelection against the chance of being caught and punished and losing an election with a tarnished reputation. Factors affecting this decision include campaign financing mechanisms, information access by voters, the ability of citizens to vote out corrupt legislators, the degree of political contestability, electoral systems, democratic institutions, and traditions and institutions of accountability in governance. Examples of such analyses include Rose-Ackerman (1978), Andvig and Moene (1990), Grossman and Helpman (1994), Flatters and Macleod (1995), Chand and Moene (1997), Van Rijckeghem and Weder (1997), and Acconcia, D'Amato, and Martina (2003). This conceptual framework is useful in analyzing political corruption or state capture.

There is a fine line dividing theoretical models that focus on the effects of localization on corruption and those that analyze the decentralization of corruption within a multitier hierarchy from an "industrial organization of corruption" type of framework. In the latter group a distinction is made between top-down corruption—where corrupt high levels buy lower levels by sharing a portion of gains—and bottom-up corruption—where low-level officials share their own collected bribes with superior levels to avoid detection or punishment. The former phenomenon is more likely to exist in a federal system of governance where powers may be shared among various orders of government and the latter is more likely to prevail under unitary or centralized forms of governance or dictatorial regimes. The impact of governance on the corruption networks is an interesting yet unresearched topic. Tirole (1986) analyzed one aspect of this network by means of a three-tier principal-supervisor-agent model (see also Guriev 1999). This extension of a conventional principal-agent model assists in drawing inferences regarding the type of corrupt relations that could evolve under a three-tier unitary government structure. These inferences are highly sensitive to underlying assumptions regarding principal-agent relationships under a multitiered system of governance. Four-tier hierarchies are modeled by Carillo (2000) and Bac and Bag (1998). In Guriev's three-tier hierarchy model the midlevel bureaucrat supervises the agent and reports to the principal. In comparing the characteristics of equilibriums with top-, bottom-, and all-level corruption, Guriev concludes that top-level

corruption "is not efficient, as it redistributes rents in favor of agents, and therefore makes it more attractive for potential entrants" (p. 2), thereby leading to higher total corruption.

Shleifer and Vishny (1993) utilize conventional industrial organization theory model and conclude that decentralization is likely to increase corruption. In this model, government bureaucracies and agencies act as monopolists selling complimentary government-produced goods that are legally required for private-sector activity. The main idea behind the model is that under centralized corruption, bureaucracies act like a joint monopoly, whereas under decentralized corruption, bureaucracies behave as independent monopolies. When bureaucracies act as independent monopolies, they ignore the effects of higher prices on the overall demand for a good and hence drive up the cumulative bribe burden.

Waller, Verdier, and Gardner (2002) define decentralized corruption as a system in which higher-level officials collect a fixed amount of bribe income from each of the bureaucrats who take bribes, without mandating the bribe size that the bureaucrats charge. In a centralized system, on the contrary, bribe size is determined by the higher level of government, which collects it from bureaucrats and redistributes it among them after keeping a share. Waller et al. posit that decentralized corruption leads to lower levels of total corruption in the economy (lower spread), higher levels of bribe per entrepreneur (higher depth), and a smaller formal sector vis-à-vis a centralized corruption equilibrium. Yet, these results vary widely for specific regimes in the model when given parameters satisfy key conditions; for instance, for high-enough wages and monitoring systems, centralized corruption may reduce total corruption and expand the formal economy.

While previously discussed studies centered on the organizational structure of corruption, Ahlin (2001) differs by concentrating on the alternative effects of different types of decentralization, and doing so from a horizontal, as opposed to hierarchical, perspective. In this model, a country is divided in regions, each with a given number of independent power groups. *Bureaucratic decentralization* affects the political organization in a region by increasing the number of power groups or bureaucracies, while the number of jurisdictions captures the degree of *regional decentralization* (i.e., having a single region and bureaucracy would reflect the maximum degree of centralization). Ahlin's theoretical results suggest that corruption is determined by mobility of economic agents across regions. Under the assumption of no interregional mobility, corruption increases with the degree of bureaucratic decentralization but is independent of the degree of regional decentralization, whereas for perfect interregional mobility, corruption decreases with regional decentralization and is independent of bureaucratic decentralization. A key intuition of the model is that corrupt bureaucrats fail to internalize the costs of increases in bribe charges imposed on other bureaucrats.

Arikan (2004) uses a tax competition framework to examine localization-corruption links. In his model, corruption is measured as the proportion of tax

revenue appropriated by bureaucrats, whereas decentralization is captured by the number of jurisdictions competing for a mobile tax base. Local governments decide on the levels of tax rates and corrupt earnings in order to maximize a weighted sum of corrupt earnings and citizens' utility. In this framework, a higher degree of decentralization is expected to lead to lower levels of corruption.

Bardhan and Mookherjee (2000) shed light on the determinants of capture of the democratic process. Not surprisingly, they conclude that the extent of relative capture is ambiguous and context specific. They find that the extent of capture at the local level depends on the degree of voter awareness, interest group cohesiveness, electoral uncertainty, electoral competition, and the heterogeneity of interdistrict income inequality. A key assumption of this model is that the degree of political awareness is correlated to education and socioeconomic position—in particular, that the fraction of informed voters in the middle income class is lower than or equal to that of the rich, and higher than that of the poor. Uninformed voters are swayed by campaign financing, whereas informed voters favor the party platform that maximizes their own-class utility. The outcome of local and national elections in terms of policy platforms will coincide under four assumptions: (1) all districts have the same socioeconomic composition, and swings among districts (particular district-specific preferences for one of two political parties) are perfectly correlated; (2) national elections are majoritarian; (3) there is an equal proportion of informed voters in local and national elections; and (4) the proportion of rich who contribute to their lobby is equal at the national and local levels—the rich are as well organized nationally as locally. Alternatively, capture will be higher at the local level if conditions (3) and (4) fail—that is, if the proportion of informed voters is lower at the national levels and the rich are less organized nationally than they are locally. On the contrary, greater electoral uncertainty at the local level due to differences in the electoral competition implies lower capture at the local level. This would be the case if, for example, swings are not identical but rather drawn from the same distribution across districts (assuming this distribution satisfies a regularity condition); heterogeneity on swings will favor different parties, implying less capture of the nationally dominant party.

No definitive conclusions can be drawn regarding corruption and the centralization-decentralization nexus from the agency type of conceptual models. These models simply reaffirm that the incidence of corruption is context dependent and therefore cannot be uncovered by generalized models.

(ii) New Public Management Frameworks. The new public management (NPM) literature points to a more fundamental discordance among the public sector mandate, its authorizing environment, and the operational culture and capacity. According to NPM, this discordance contributes to government acting like a runaway train and government officials indulging in rent-seeking behaviors with little opportunity for citizens to constrain government behavior. This viewpoint calls

for fundamental civil service and political reforms to create a government under contract and accountable for results. Public officials will no longer have permanent rotating appointments but instead they could keep their jobs as long as they fulfilled their contractual obligations (see Shah 1999, 2005).

The NPM paradigms have clear implications for the study of localization and corruption as it argues for contractual arrangements in provision of public services. Such a contractual framework may encourage competitive service delivery through outsourcing, with purchaser-provider split under a decentralized structure of governance. The NPM goals are harmonious with localization as greater accountability for results reinforces government accountability to citizens through voice and exit mechanisms. Conceptually, therefore, NPM is expected to reduce opportunities for corruption (see Shah 1999, 2005; VonMaravic 2003). Andrews and Shah (2005) integrate these two ideas in a common framework of citizen-centered governance. They argue that citizen empowerment holds the key to enhanced accountability and reduced opportunities for corruption.

Others disagree with such conclusions and argue that that NPM could lead to higher corruption as opposed to greater accountability. This may happen because the tendering for service delivery and separation of purchasers from providers may lead to increased rent-seeking behaviors and enhanced possibilities for corruption (Batley 1999; Von Maravic 2003). Further, some argue that decentralized management leads to weaker vertical supervision from higher levels and the inadequacy of mechanisms to exert controls over decentralized agencies (Scharpf 1997). This loss in vertical accountability is seen as a source of enhanced opportunities for corruption. Of course, this viewpoint simply neglects potential gains from higher horizontal accountability.

(iii) Neo-Institutional Economics (NIE) Frameworks. Finally, neo-institutional economics (NIE) presents a refreshing perspective on the causes and cures of corruption. The NIE approach argues that corruption results from opportunistic behavior of public officials, as citizens either are not empowered or face high transaction costs to hold public officials accountable for their corrupt acts. The NIE treats citizens as principals and public officials as agents. The principals have bounded rationality—they act rationally based on the incomplete information they have. In order to have a more informed perspective on public sector operations, they face high transaction costs in acquiring and processing the information. Agents (public officials) are better informed. This asymmetry of information allows agents to indulge in opportunistic behavior, which goes unchecked due to high transaction costs faced by the principals and a lack of or inadequacy of countervailing institutions to enforce accountable governance.[4] Thus corrupt countries have inadequate mechanisms for contract enforcement, weak judicial systems, and inadequate provision for public safety. This raises the transaction costs in the economy, further raising the cost of private capital as well as the cost of public service provision. The problem is further compounded by

path dependency (i.e., a major break with the past is difficult to achieve, as any major reforms are likely to be blocked by influential interest groups); cultural and historical factors; and mental models where those who are victimized by corruption feel that attempts to deal with corruption will lead to further victimization, with little hope of corrupt actors being brought to justice. These considerations lead principals to the conclusion that any attempt on their part to constrain corrupt behaviors will invite strong retaliation from powerful interests. Therefore, citizen empowerment (e.g., through devolution, citizens' charter, bill of rights, elections, and other forms of civic engagement) assumes critical importance in combating corruption because it may have a significant impact on the incentives faced by public officials to be responsive to public interests.

(b) EMPIRICAL PERSPECTIVES. The empirical literature on this subject lends support to the NIE perspective elaborated in the preceding subsection but goes beyond to identify some key drivers based on in-depth country studies—including a recent World Bank look at Guatemala, Kenya, Latvia, Pakistan, the Philippines, and Tanzania—and econometric studies of developing, transition, and industrial countries (see World Bank 2004; Tomaszewska and Shah 2000; Gurgur and Shah 2002; Huther and Shah 2000). The six country case studies by the World Bank examined the root causes of corruption and evaluated the impact of World Bank efforts to reduce corruption in each country. The key corruption drivers identified by these studies include:

- *The legitimacy of the state as the guardian of the public interest is contested*. In highly corrupt countries, there is little public acceptance of the notion that the role of the state is to rise above private interests to protect the broader public interest. Clientelism—public officeholders focusing on serving particular client groups linked to them by ethnic, geographic, or other ties—shapes the public landscape and creates conditions that are ripe for corruption. The line between what is public and what is private is blurred so that abuse of public office for private gain is a routine occurrence.
- *The rule of law is weakly embedded*. Public-sector corruption thrives where laws apply to some but not to others, and where enforcement of the law is often used as a device for furthering private interests rather than protecting the public interest. A common symbol of the breakdown of the rule of law in highly corrupt countries is the police acting as lawbreakers rather than law enforcers—for example, stopping motorists for invented traffic violations as an excuse for extracting bribes. As well, the independence of the judiciary—a pillar of the rule of law—is usually deeply compromised in highly corrupt countries.
- *Institutions of participation and accountability are ineffective*. In societies where the level of public-sector corruption is relatively low, one normally finds strong institutions of participation and accountability that control

abuses of power by public officials. These institutions either are created by the state itself (for example, electoral process, citizens' charter, bill of rights, auditors-general, the judiciary, the legislature) or arise outside of formal state structures (for example, the news media and organized civic groups). There are glaring weaknesses in institutions of participation and accountability in highly corrupt countries.

- *The commitment of national leaders to combating corruption is weak*. Widespread corruption endures in the public sector when national authorities are either unwilling or unable to address it forcefully. In societies where public-sector corruption is endemic, it is reasonable to suspect that it touches the highest levels of government, and that many senior officeholders will not be motivated to work against it.

(i) How to Formulate a Strategy. So what can policymakers do to combat corruption? Experience strongly suggests that the answer lies in taking an indirect approach and starting with the root causes. To understand why, it is helpful to look at a model that divides developing countries into three broad categories—high, medium, and low—reflecting the incidence of corruption. The model also assumes that countries with high corruption have a poor quality of governance, those with medium corruption have fair governance, and those with low corruption have good governance. (See Exhibit 10.1.)

What this model reveals is that because corruption is itself a symptom of fundamental governance failure, the higher the incidence of corruption, the *less* an anticorruption strategy should include tactics that are narrowly targeted to corrupt behaviors and the *more* it should focus on the broad underlying features of the governance environment. For example, support for anticorruption agencies and public awareness campaigns is likely to meet with limited success in environments

Incidence of Corruption	Quality of Governance	Priorities of Anticorruption Efforts
High	Poor	Establish rule of law; strengthen institutions of participation and accountability; establish citizens' charter; limit government intervention; implement economic policy reforms
Medium	Fair	Decentralize and reform economic policies and public management; introduce accountability for results
Low	Good	Establish anticorruption agencies; strengthen financial accountability; raise public and official awareness; make antibribery pledges; conduct high-profile prosecutions

EXHIBIT 10.1 ONE SIZE DOES NOT FIT ALL: EFFECTIVE ANTICORRUPTION POLICIES SPECIFY A PECKING ORDER OF REFORMS BASED ON A RECOGNITION OF THE BROADER INSTITUTIONAL ENVIRONMENT IN EACH COUNTRY

where corruption is rampant and the governance environment deeply flawed. In fact, in environments where governance is weak, anticorruption agencies are prone to being misused as tools of political victimization. These types of interventions are more appropriate to a low-corruption setting, where one can take for granted (more or less) that the governance fundamentals are reasonably sound and that corruption is a relatively marginal phenomenon.

The model also suggests that where corruption is high (and the quality of governance is correspondingly low), it makes more sense to focus on the underlying drivers of malfeasance in the public sector—for example, by building the rule of law and strengthening institutions of accountability. Indeed, a lack of democratic institutions (a key component of accountability) has been shown to be one of the most important determinants of corruption (Gurgur and Shah 2002). When Malaysia adopted a clients' charter in the early 1990s that specified service standards and citizens' recourse in the event of noncompliance by government agencies, it helped reorient the public sector toward service delivery and transform the culture of governance (Shah 1999, 2005).

In societies where the level of corruption lies somewhere in between the high and low cases, it may be advisable to attempt reforms that assume a modicum of governance capacity—such as trying to make civil servants more accountable for results, bringing government decision making closer to citizens through decentralization, simplifying administrative procedures, and reducing discretion for simple government tasks such as the distribution of licenses and permits.

(ii) Insights into Past Failures. With this model in mind, it is not hard to understand why so many anticorruption initiatives have met with so little success (see Exhibit 10.2 for a summary of the empirical evidence). Take, for example, the almost universal failure of wide-ranging media awareness campaigns, and of seminars and workshops on corruption targeted to government officials, parliamentarians, and journalists. As the model shows, this outcome would be expected in countries with weak governance, where corruption is openly practiced but neither the general public nor honest public officials feel empowered to take a stand against it and even fear being victimized. In contrast, awareness campaigns would be expected to have a positive impact in countries where governance is fair or good and the incidence of corruption is low.

Decentralization provides a further illustration of the importance of understanding the circumstances in which corruption occurs. There is indeed evidence that decentralization can be an effective antidote to corruption because it increases the accountability of public authorities to citizens; for additional references and evidence, see Gurgur and Shah (2002) and Shah, Thompson, and Zou (2004). However, decentralization creates hundreds of new public authorities, each having powers to tax, spend, and regulate that are liable to being abused in environments where governance is weak. As the World Bank's analysis of the Philippines in the

Program	Empirical Evidence
Anticorruption Agencies	Anticorruption agencies have been successful in Chile, Hong Kong, New South Wales, Australia, and Singapore (Allan 1992; Clark 1987; Holm 2000; Doig 1995; Klitgaard 1998; Segal 1999; World Bank 1999). Developing country officials, however, do not see these as effective anticorruption tools in countries with endemic corruption (see Kaufmann 1997).
Public Opinion Surveys	Public opinion surveys have served as a useful tool in articulating more precisely citizens' concerns (e.g., Bangalore scorecard and a ''corruptometer'' by an Argentine NGO). International surveys, such as those compiled by Transparency International, highlight countries in which corruption is perceived to be endemic.
Raising Public Sector Wages	Rijckeghem and Weder (1997) find no short-run impact (as the income from bribery dominates total income). Gurgur and Shah (1999, 2000) find negative yet insignificant effect. Treisman (1999) and Swamy et al. (1999) find no relationship. The SDC experience in the forestry sector in Pakistan also confirms this. In corrupt societies public positions are often purchased by borrowing money from family and friends. Raising public sector wages simply raises the purchase price and subsequent corruption efforts to repay loans. Of course, raising public sector wages, which do not allow employees to satisfy basic needs of their families, is likely to reduce petty corruption.
Reducing Public Sector Size	Tanzi and Davoodi (1998), LaPalombara (1994), and La Porta et al. (1999) find that reduction in public sector size leads to less corruption. Gurgur and Shah (1999) find that this result holds only when important variables such as the judiciary, democratic institutions, colonial heritage, decentralization, and bureaucratic culture are omitted. Elliot (1997) finds an inverse relationship between the budget size and corruption. Privatization in some countries (e.g., Russia) has led to increased corruption and exploitation. Thus the appropriate role of the government is the critical element for a discussion on corruption.
Financial Accountability	Gurgur and Shah (1999, 2000) find a negative yet insignificant association.
Media Independence	Freedom of the press is negatively correlated with the level of corruption (see Brunetti and Weder 1998).
Judicial Independence	Judicial independence reduces corruption, as confirmed by Ades and Di Tella (1996), Goel and Nelson (1998), and Gurgur and Shah (1999, 2000).
Citizen Participation	Citizen participation leads to reduced corruption, as confirmed by Kaufman and Sachs (1998), and Gurgur and Shah (1999, 2000).
Decentralization	Huther and Shah (1998), Gurgur and Shah (2000), and Fisman and Gatti (2000) find a negative relationship between decentralization and corruption.
Bureaucratic Culture	Gurgur and Shah (1999, 2000) find a positive relationship between command-and-control type civil service orientation and corruption.

Source: Huther and Shah (2000).

EXHIBIT 10.2 EMPIRICAL EVIDENCE ON SELECTED ANTICORRUPTION PROGRAMS

1990s has shown, decentralization may multiply rather than limit opportunities for corruption if it is implemented under the wrong circumstances. This issue is the central theme of this chapter, and it is analyzed further in the following sections.

As for raising civil service salaries and reducing wage compression—the ratio between the salaries of the highest- and lowest-paid civil servants in a given country—again, the model provides some insights. The evidence suggests that in environments where governance is weak, wage-based strategies are not likely to have a significant impact on civil service corruption; see Huther and Shah (2000) for references. Moreover, reducing wage compression may even encourage corruption if public sector positions are viewed as a lucrative career option. For instance, in corrupt societies public positions are often purchased by borrowing money from family and friends. Raising public sector wages simply raises the purchase price and subsequent corruption efforts to repay loans.

How about the establishment of watchdog agencies—something most developing countries have done—with a mandate to detect and prosecute corrupt acts? Here, too, the governance-corruption nexus is key. Watchdog agencies have achieved success only in countries where governance is generally good, such as Australia and Chile. In weak governance environments, however, these agencies often lack credibility and may even extort rents. In Kenya, Malawi, Sierra Leone, Tanzania, Uganda, and Nigeria, for example, anticorruption agencies have been ineffective. In Tanzania, the government's Prevention of Corruption Bureau produces only about six convictions a year, mostly against low-level functionaries, in a public sector environment rife with corruption. In Pakistan, the National Accountability Bureau does not even have a mandate to investigate corruption in the powerful and influential military. Ethics offices and ombudsmen have had no more success than anticorruption agencies in countries where governance is poor (see Huther and Shah 2000; Shah and Schacter 2004).

The preceding discussion confirms the policy conclusions of Exhibit 10.1 that due recognition of the initial conditions is important for the effectiveness of anticorruption policies, and commonly pursued anticorruption strategies are unlikely to succeed if they do not recognize the pecking order of reforms in a poor governance environment. Exhibit 10.3 provides guidance on the relevance of commonly pursued policies under different governance environments.

10.4 CONCLUSIONS: DON'T USE THE "C" WORD

Both the conceptual guidance and empirical guidance offer the same clue on the causes of a losing battle against corruption—policy makers too often use the "C" word (corruption) and focus directly on dealing with the symptoms while ignoring the broader disease of dysfunctional governance. It is only the latter focus that is likely to make a difference in the fight against corruption in the long

Program	Country's Quality of Governance			Comments
	Weak	Fair	Good	
Raising Public Awareness of Corruption through Seminars	Not relevant	Low	Medium	In countries with weak governance, corrupt practices and agents are generally well known.
Raising Awareness of Public Officials through Seminars	Not relevant	Low	Medium	Public officials may be aware of corruption but unwilling and/or unable to take action due to incentive problems in countries with weak governance.
Anticorruption Agencies/ Ombudsman	Not relevant	Low	Medium	With endemic corruption, anticorruption agencies or ombudsman may actually extort rents. Positive influence if preconditions for good governance exist.
Ethics Office	Not relevant	Low	Medium	Positive influence may be limited to societies with good governance.
Raising Public Sector Wages	Negligible	Low	Medium	May have positive impact on petty corruption but little impact on grand corruption. Negative impact if part of the problem is excessive public employment.
Reducing Wage Compression	Negligible	Negligible	Negligible	More relevant as an incentive mechanism for career development. May increase corruption if the public sector is viewed as a lucrative career option by greedy elements of society.
Merit-Based Civil Service	Low	Medium	High	May be derailed by bureaucratic processes in highly corrupt societies.
Public Opinion Surveys	Low	Medium	Medium	Public opinion surveys have served as a useful tool in articulating citizens' concerns (e.g., Bangalore scorecard).
Financial Accountability	Low	Low	Medium	Appropriate when democratic accountability and a substantial accounting/bookkeeping infrastructure with some integrity are in place.
Parliamentary Oversight	Low	Medium	Medium	Parliamentary oversight can be helpful, but parliamentary micromanagement is not an effective form of governance.

EXHIBIT 10.3 RATINGS ON RELEVANCE OF A MENU OF ANTICORRUPTION PROGRAMS

Program	Country's Quality of Governance			Comments
	Weak	Fair	Good	
Reducing Public Employment	Medium	Low	Low	May reduce opportunities for corruption.
Decentralization	Medium	Low	Low	May improve accountability and may increase sense of social purpose for public officials.
Client-Based Civil Service/ Bureaucratic Culture	Medium	Medium	Low	Success depends on service delivery orientation of public service, reinforced by accountability for results.
Economic Policy Reform	High	Medium	Low	Reduces potential corruption by shifting decision making to the private sector.
Media and Judicial Independence, Citizen Participation	High	Medium	Low	Allows for detection, followed by accountability.
Reducing Public Sector Size	High	Medium	Low	By reducing the number of government activities, officials can focus on primary objectives of the state.
Rule of Law	High	Medium	Low	Essential for any progress.

Source: Huther and Shah (2000).

EXHIBIT 10.3 (*continued*) RATINGS ON RELEVANCE OF A MENU OF ANTICORRUPTION PROGRAMS

run. The following considerations may be helpful in designing and implementing anticorruption strategies.

- *Pecking order of reforms.* Because corruption is a system of failed governance, the higher the incidence of corruption, the less an anticorruption strategy should include tactics that are narrowly targeted to corrupt behaviors and more it should focus on the broad underlying features of the governance environment. This suggests a pecking order of reforms in highly corrupt countries. The order of priorities in these countries should be to first establish the rule of law, strengthen the institutions of participation and accountability, and establish citizens' charters defining basic legal rights, including access to defined public services standards. Limiting government interventions and implementation of economic policy reforms should be part of this package. The second priority should be to clarify the roles and responsibilities of various orders of government and introduce performance-based accountability to hold government to account for service delivery performance. The third priority would be to implement policies dealing with detection and punishment of corrupt acts.

- *Service delivery performance.* Any serious effort by domestic and external stakeholders to hold governments to service delivery standards will eventually compel those governments to address the causes and consequences of corruption. Also, given the difficulty of detecting corruption through financial audits, corruption may be more easily detected through observation of public service delivery performance. Malaysia's clients' charter represents an important innovation to empower citizens to hold government to account for delivery of defined service standards.
- *Citizen empowerment through support for bottom-up reforms.* In many countries where corruption is entrenched, governments lack either the will or the capability to mount effective anticorruption programs. Internal and external stakeholders may choose to amplify citizens' voice and strengthen exit mechanisms so as to enhance transparency, accountability, and the rule of law. Strengthening local governance and establishing home rule may be an important tool in this regard.
- *Information dissemination.* Letting the sun shine on government operations is a powerful antidote to corruption. The more influence donors can exert on strengthening citizens' right to know and on governments to release timely, complete, and accurate information about government operations, the better the prospects for reducing corruption. Information about how governments spend money and manage programs, and about what these programs deliver in services to people, is a key ingredient of accountability, which in turn may be an important brake on corruption.
- *Economic policy reform.* Trade and financial liberalization can reduce opportunities for corruption by limiting the situations where officials might exercise unaccountable discretionary powers, by introducing transparency, and by limiting public-sector monopoly powers.

Notes

1. This chapter is based on the author's earlier paper, "Fighting Corruption in Developing Countries: Insights from the Past Failures."
2. This section draws upon Shah and Schacter (2004).
3. For comprehensive surveys on corruption, see Jain (2001) and Aidt (2003).
4. Following this line of thought, Lambsdorff et al. note that in fighting corruption from an NIE perspective, policy makers should aim to "encourage betrayal among corrupt parties, to destabilize corrupt agreements, to disallow corrupt contracts to be legally enforced, to hinder the operation of corrupt middlemen, and to find clearer ways of regulating conflicts of interest."

References

Abed, George T., and Hamid Davoodi. 2000. Corruption, structural reforms, and economic performance in the transition economies. International Monetary Fund Working Paper 00/132.

Acconcia, Antonio, Marcello D'Amato, and Riccardo Martina. 2003. Corruption and tax evasion with competitive bribes. CSEF Working Paper 112, Centre for Studies in Economics and Finance, University of Salerno, Italy.

Ades, Alberto, and Rafael Di Tella. 1997. National champions and corruption: Some unpleasant interventionist arithmetic. *Economic Journal* 107: 1023–1042.

Ahlin, Christian. 2000. Corruption, aggregate economic activity and political organization. University of Chicago, processed.

Ahlin, Christian. 2001. Corruption: Political determinants and macroeconomic effects. Working Paper 01-W26, Department of Economics, Vanderbilt University.

Aidt, Toke S. 2003 Economic analysis of corruption: a survey, *The Economic Journal* Volume 113 Issue 491 November 2003.

Andrews, Matthew, and Anwar Shah. 2005. Citizen-centered governance: A new approach to public sector reform. Chapter 6, 152–182. Towards citizen-centered local budgets in developing countries. Chapter 7, 183–216. In *Public expenditure analysis*, ed. Anwar Shah. Washington, DC: World Bank.

Andvig, Jens Chr., and Karl O. Moene. 1990. How corruption may corrupt. *Journal of Economic Behavior and Organization* 13: 63–76.

Arikan, Gulsun. 2000. Fiscal decentralization: A remedy for corruption? Department of Economics, University of Illinois at Urbana-Champaign, processed.

Arikan, Gulsun. 2004. Fiscal decentralization: A remedy for corruption? *International Tax and Public Finance* 11: 175–195.

Bac, Mehmet, and Parimal K. Bag. 1998. Corruption, collusion and implementation: A hierarchical design. Mimeo, University of Liverpool, UK.

Banfield, Edward. 1975. Corruption as feature of government organization. *Journal of Law and Economics* 18: 587–695.

Bardhan, Pranab. 1997. Corruption and development: A review of issues. *Journal of Economic Literature* 35 (September): 1320–1346.

Bardhan, Pranab, and Dilip Mookherjee. 2000. Decentralizing anti-poverty program delivery in developing countries. Working paper, University of California, Berkeley.

Batley, R. 1999. The role of government in adjusting economies: An overview of findings. International Development Department, University of Birmingham, Birmingham, Alabama.

Becker, Gary Stanley. 1968. Crime and punishment: An economic approach. *Journal of Political Economy* 76 (2): 169–217.

Becker, Gary Stanley. 1983. A theory of competition among pressure groups for political influence. *Quarterly Journal of Economics* 97 (3): 371–400.

Becker, Gary Stanley, and George Stigler. 1974. Law enforcement, malfeasance and the compensation of enforcers. *Journal of Legal Studies* 3: 1–19.

Blanchard, Olivier, and Andrei Shleifer. 2000. Federalism with and without political centralization: China versus Russia. Working Paper 7616, National Bureau of Economic Research (March): 1–14.

Carbonara, Emanuela. 1999. Bureaucracy, corruption and decentralization. Department of Economics Working Paper 342/33, University of Bologna, Italy.

Carillo, Juan D. 2000. Corruption in hierarchies. *Annales d'Economie et de Statistique* (Institut National de la Statistique et des Etudes Economiques, France) 59: 37–61.

Chand, Sheetal K., and Karl O. Moene. 1997. Controlling fiscal corruption. International Monetary Fund Working Paper WP/97/100.

Crook, Richard, and James Manor. 2000. Democratic decentralization. OED Working Paper 11 (Summer 2000), World Bank, Washington, DC.

De Mello, Luis, and Matias Barenstein. 2001. Fiscal decentralization and governance—A cross-country analysis. International Monetary Fund Working Paper 01/71.

Fisman, Raymond, and Roberta Gatti. 2002. Decentralization and corruption: Evidence across countries. *Journal of Public Economics* 83: 325–345.

Fiszbein, Ariel. 1997. Emergence of local capacity: Lessons from Colombia. *World Development* 25 (7): 1029–1043.

Flatters, Frank, and W. Bentley Macleod. 1995. Administrative corruption and taxation. *International Tax and Public Finance* 2: 397–417.

Grossman, Gene M., and Elhanan Helpman. 1994. Protection for sale. *American Economic Review* 84 (4): 833–850.

Gupta, Sanjeev, Hamid Davoodi, and Rosa Alonso-Terme. 1998. Does corruption affect income inequality and poverty? International Monetary Fund Working Paper 98/76.

Gupta, Sanjeev, Hamid Davoodi, and Erwin Tiongson. 2000. Corruption and the provision of health care and education services. International Monetary Fund Working Paper 00/116.

Gurgur, Tugrul, and Anwar Shah. 2002. Localization and corruption: Panacea or Pandora's box? In *Managing fiscal decentralization*, ed. Ehtisham Ahmad and Vito Tanzi, 46–67. London and New York: Routledge Press.

Guriev, Sergei. 1999. A theory of informative red tape with an application to top-level corruption. Working Paper #99/007. Moscow, Russia: New Economic School.

Guriev, Sergei. 2003. Red tape and corruption. Discussion Paper 3972, Centre for Economic Policy Research, UK: 1–27.

Huther, Jeff, and Anwar Shah. 1998. Applying a simple measure of good governance to the debate on fiscal decentralization. Policy Research Working Paper 1894, World Bank, Washington, DC.

Huther, Jeff, and Anwar Shah. 2000. Anti-corruption policies and programs: A framework for evaluation. Policy Research Working Paper 2501, World Bank, Washington, DC.

Jain, Arvind K. 2001. Corruption: A Review, *Journal of Economic Surveys,* Volume 15 Issue 1, February 2001.

Klitgaard, Robert E. 1988. *Controlling corruption*. Berkeley: University of California Press.

Klitgaard, Robert E. 1991. Gifts and bribes. In *Strategy and choice*, ed. Richard Zeckhauser. Cambridge, MA: MIT Press.

Kuncoro, Ari. 2000. The impact of licensing decentralization on firm location choice: The case of Indonesia. Faculty of Economics, University of Indonesia, processed.

Lambsdorff, Johann. 1999. Corruption in empirical research—A review. Transparency International, processed.

Mauro, Paolo. 1995. Corruption and growth. *Quarterly Journal of Economics* 110 (3): 681–713.

Olowu, Dele. 1993. Roots and remedies of government corruption in Africa. *Corruption and Reform* 7 (3): 227–236.

Prud'homme, Remy. 1994. On the dangers of decentralization. Policy Research Working Paper 1252, World Bank, Washington, DC.

Rose-Ackerman, S. 1975. The economics of corruption. *Journal of Public Economics* 4 (February): 187–203.

Rose-Ackerman, S. 1978. *Corruption: A study in political economy*. New York: Academic Press.

Scharpf, Fritz W. 1997. Games real actors play—Actor-centered institutionalism in policy research. Boulder, CO: Westview Print.

Seabright, Paul. 1996. Accountability and decentralization in government: An incomplete contracts model. *European Economic Review* 40 (1): 61–89.

Shah, Anwar. 1998. Balance, accountability, and responsiveness: Lessons about decentralization. Policy Research Working Paper 2021 (December), World Bank, Washington, DC.

Shah, Anwar. 1999. Governing for results in a globalized and localized world. *Pakistan Development Review* 38 (4), Part I: 385–431.

Shah, Anwar. 2005. On getting the giant to kneel: Approaches to a change in the bureaucratic culture. In *Fiscal management*, ed. Anwar Shah, Public Sector Governance and Accountability Series, 211–229. Washington, DC: World Bank.

Shah, Anwar. 2006. Corruption and decentralized public governance. In *Handbook of fiscal federalism*, ed. Ehtisham Ahmad and Giorgio Brosio, Chapter 19, 478–498. Cheltenham, UK and Northampton, MA: Edward Elgar.

Shah, Anwar, and Mark Schacter. 2004. Combating corruption: Look before you leap. *Finance and Development* 41 (4) (December): 40–43.

Shah, Anwar, Theresa Thompson, and Heng-fu Zou. 2004. The impact of decentralization on service delivery, corruption, fiscal management and growth in developing and emerging market economies: A synthesis of empirical evidence. CESifo Dice Report, *Quarterly Journal for Institutional Comparisons* 2 (Spring): 10–14.

Shleifer, Andrei, and Robert W. Vishny. 1993. Corruption. *Quarterly Journal of Economics* 108 (August): 599–617.

Tanzi, Vito. 1995. Fiscal federalism and decentralization: A review of some efficiency and macroeconomic aspects. Annual World Bank Conference on Development Economics, 295–316.

Tanzi, Vito, and Hamid Davoodi. 1997. Corruption, public investment, and growth. International Monetary Fund Working Paper 97/139.

Tirole, Jean. 1986. Hierarchies and bureaucracies: On the role of collusion in organizations. *Journal of Law, Economics, and Organization* 2: 181–214.

Tirole, Jean, and Jean-Jacques Laffont. 1988. Politics of government decision-making: A theory of regulatory capture. Working Paper 506, Department of Economics, Massachusetts Institute of Technology: 1–48.

Tomaszewska, Ewa, and Anwar Shah. 2000. Phantom hospitals, ghost schools and roads to nowhere: The impact of corruption on public service delivery performance in developing countries. Working paper, Operations Evaluation Department, World Bank, Washington, DC.

Treisman, Daniel S. 1999. *After the deluge: Regional crises and political consolidation in Russia*. Ann Arbor: University of Michigan Press.

Treisman. Daniel S. 2000. The causes of corruption: A cross-national study, *Journal of Public Economics* 76 (3) (June): 399–457.

Treisman, Daniel S., and Andrei Shleifer. 2002. A normal country. Working Paper 10057, National Bureau of Economic Research (October): 1–46.

Van Rijckeghem, Caroline, and Beatrice Weder. 1997. Corruption and the role of temptation: Do low wages in civil service cause corruption? International Monetary Fund Working Paper WP/97/73.

Van Rijckeghem, Caroline, and Beatrice Weder. 2001. Bureaucratic corruption and the rate of temptation: Do low wages in civil service cause corruption? *Journal of Development Economics* 65: 307–331.

Von Maravic, Patrick. 2003. How to analyse corruption in the context of public management reform? Paper presented at the first meeting of the Study Group on Ethics and Integrity of Governance EGPA Conference, September 2003, Portugal.

Wade, Robert. 1997. How infrastructure agencies motivate staff: Canal irrigation in India and the Republic of Korea. In *Infrastructure strategies in East Asia*, ed. Ashoka Mody. Washington, DC: World Bank.

Waller, Christopher J., Thierry A. Verdier, and Roy Gardner. 2002. Corruption: Top-down or bottom-up. *Economic Inquiry* 40 (4): 688–703.

Weinsgast, Barry. 1995. The economic role of political institutions: Market-preserving federalism and economic growth. *Journal of Law, Economics, and Organization* 11: 1–31.

Wildasin, David. 1995. Comment on "Fiscal Federalism and Decentralization." Annual World Bank Conference on Development Economics, 323–328.

World Bank. 2004. *Mainstreaming anti-corruption activities in World Bank assistance—A review of progress since 1997*. Washington, DC: World Bank.

PART 2

IT GOVERNANCE

CHAPTER 11

IT GOVERNANCE OVERVIEW

Alan Calder

In the twenty-first century, information technology (IT) governance is, within the broader corporate governance context, critical for all organizations. Organizations and enterprises without an IT governance strategy face significant risks in the short, medium, and long term; those with an IT governance strategy do perform measurably better.

11.1 GOVERNANCE BACKGROUND

The "greed is good" business philosophy of the 1980s and 1990s seemed to give way, at the end of the twentieth century, to a "looting is good" approach. Catastrophic financial failure is, of course, a characteristic of the business cycle. Looting has happened before: The Bank of Credit and Commerce International (BCCI) and Maxwell Communications in the United Kingdom are good examples. Corporate collapse, originating in a failure of internal control, has happened before: Barings Bank is an instance.

The spate of collapses and financial failures at the end of the Internet bubble, though, suggested a systemic weakness, and one whose evidently worldwide implications had a significant, negative knock-on effect on already problematic pension funds and pensioner assets. The convictions of CEOs and their advisors is evidence that Enron, WorldCom, Parmalat, and many other corporate disasters were the storm damage of unbridled executive authority; shareholders are not enthusiastic about losses on this scale.

Governments, already grappling with the challenge of funding the pensions of the inexorably graying baby boomer bulge, are aware that they cannot afford further wanton asset destruction in the private sector. They have therefore raised their focus on rooting out corporate misbehavior. Eliot Spitzer, the New York attorney general, expressed a not uncommon view when he said, "The honor code among CEOs didn't work. Board oversight didn't work. Self-regulation was a complete failure."[1]

They are doing this through a combination of overt regulatory action and slightly more covert pressure on institutional investors to stand up for their rights as stockholders and more determinedly exercise their de facto responsibility to insist on proper governance from those organizations in which they are invested. Executives are, of course, resisting.

The concept of governance is a simple one: "Corporate governance is the system by which business corporations are directed and controlled."[2] The holy trinity of good corporate governance has long been seen as shareholder rights, transparency, and board accountability. While corporate governance is overtly concerned with board structure, executive compensation, and shareholder reporting, the underlying assumption is that it is the board that is responsible for managing the business and controlling the risks to its assets and trading future.

In today's corporate governance environment, where the value and importance of intellectual assets are significant, boards must be seen to extend the core governance principles—setting strategic aims, providing strategic leadership, overseeing and monitoring the performance of executive management, and reporting to shareholders on their stewardship of the organization—to the organization's intellectual capital, information, and IT. A culture of opaqueness is out of line with today's expectation of proactive boards and governance transparency.

Boards that are not proactive in understanding the strategic importance of and operational risks in intellectual capital, information, and communications technology, are at best a drag on the effectiveness of their boards. As younger companies, controlled and managed by people who have grown up with IT and its possibilities, transform the business landscape, those boards that fail to respond can expect their businesses to be destroyed—and whether the destruction is piece by piece or wholesale is, in the long run, irrelevant.

Information technology governance is "a framework for the leadership, organizational structures and business processes, standards and compliance to

these standards, which ensure that the organization's IT supports and enables the achievement of its strategies and objectives."[3] In the future, IT governance will be even more important than corporate governance is today: Information and IT are absolutely fundamental to business survival, and organizations that fail to "direct and control" their IT to best competitive advantage will be left as roadkill on the information superhighway.

The five major drivers of IT governance are:

1. The search for competitive advantage in the dynamically changing information economy through intellectual assets, information, and IT
2. Rapidly evolving governance requirements across the Organization for Economic Cooperation and Development (OECD), underpinned by capital market and regulatory convergence
3. Increasing information- and privacy-related legislation (compliance)
4. The proliferation of threats to intellectual assets, information, and IT
5. The need to align technology projects with strategic organizational goals, ensuring they deliver planned value (project governance)

11.2 INFORMATION ECONOMY, INTELLECTUAL CAPITAL

The new information, or knowledge, economy is fundamentally different from the old manufacturing economy. The globalization of markets, products, and resources has led to increasingly similar shopping streets selling increasingly similar products throughout the developed world. In the less developed world, counterfeit versions of Western products usually sell just as well. Over 70 percent of workers in developed economies are now knowledge, rather than manual, workers, including those factory and farm workers whose work depends on understanding and using information technology. Information networking and telecommunications connectivity make this global village possible—and bring numerous other threats and challenges at the same time.

The key characteristics of the global information economy, in contrast to those of the older manufacturing one, are:

- Information and knowledge are not depleting resources to be protected; on the contrary, sharing knowledge drives innovation.
- Effects of location and time are diminished—virtual organizations now operate around the clock in virtual marketplaces, and organizations based on East Coast America manufacture in China, handle customer support from India, and sell globally through a single web site.
- Laws and taxes are difficult to apply effectively on a national basis, as knowledge quickly shifts to low-tax, low-regulation environments.
- Knowledge-enhanced products command price premiums.
- Captured knowledge has a greater intrinsic value than knowledge on the hoof.

In a very real sense, knowledge grows as it is shared; more knowledge leads to more innovation, which drives more competition, which in turn drives more globalization, and so on.

In the manufacturing economies of the nineteenth and twentieth centuries, an organization's key asset was its productive capability: its machinery, logistical support, and distribution equipment, together with its stocks of raw materials and finished goods. Risk management and asset security necessarily focused on protecting and preserving fundamentally physical assets.

In the information age, an organization's key asset is its intellectual capital: its human resources, retained knowledge, structural capital, and intangible assets. Every organization with a long-term desire to survive and succeed in its chosen market has to focus on preserving, protecting, developing, and applying its intellectual capital for the benefit of its shareholders.

Intellectual capital depends, for its productive existence, on information and communication technology: Proper IT governance is, therefore, fundamental to both the proper governance and the long-term survival of any twenty-first century organization.

11.3 COMPETITIVENESS

In 2005, Singapore displaced the United States as the top economy in information technology competitiveness, according to the World Economic Forum's *Global Information Technology Report*.[4] Iceland, Finland, and Denmark followed Singapore, knocking the United States down to fifth place after three years at the top. Information and communications technology (ICT), observed the report, is "increasingly playing the catalytic role in pushing the development process forward."

The same is true for business. IT is neither low-cost nor low-impact. It is investment-intensive. Innovation is common; speed of innovation and deployment can be critical in developing and maintaining competitive advantage. Organizations must respond proactively to change within their markets or see their competitive position eroded and ultimately destroyed.

IT on its own and of itself is not, however, necessarily a source of competitive advantage. The *way it is used* by an organization may be a source of competitive advantage, but, in many situations, IT is already commoditized and organizations have to ensure that their systems and processes are as good as (or no worse than) those of their competitors, in order to ensure they don't fall behind in key performance areas.

11.4 IT SERVICE DELIVERY

Effective IT governance, though, is mostly about the day-to-day alignment of IT activity and efforts with business goals and requirements. IT has moved way beyond the mere automation of the accounting process; it is now fundamental to the whole operation of the enterprise. All organizations should of course have an

IT strategy; critically, however, this IT strategy should be evolved only *after* the development of the business strategy, and its starting point should be a focus on using current and future IT resources to deliver the identified business objectives. The emergence, worldwide, of the concept of IT service management recognizes this fundamental truth: that the business and business users are the customers of the IT organization and that the IT organization's success depends on delivering the IT infrastructure and services that enable the business to compete effectively.

ICT makes revolutionary business models[5] possible and dramatically transforms the business environment. The fact that online security is an issue only slows down the speed with which online banking, financial services, and other e-commerce applications develop, but the final outcome is not in doubt. The Internet does enable small businesses everywhere to compete with larger ones globally; digital communication speeds up outsourcing, customer awareness, and reputation destruction. Instant messaging, voice over IP, spyware, and sequential autoresponders are technologies as disruptive as customer response management (CRM), human resource management (HRM), and Enterprise Resource Planning (ERP) systems were in their day. Of course, the Internet doesn't replace the need for a real business strategy, or for generating real economic returns for shareholders; it just transforms the environment within which the board has to create and execute strategy.

The board must govern IT—it must ensure the organization's information strategy, IT systems, and IT infrastructure are appropriate for its business model and strategic goals. A board that is not aware of how technology is transforming its business space, and that is not actively investigating how it can use technology to transform its own business (cannibalizing existing activities if appropriate) is a business for which some other organization is already creating a silver bullet.[6]

11.5 GOVERNANCE CONVERGENCE

The modern corporate governance movement arguably started with the Cadbury and Greenbury reports in the UK in the 1990s. They were merged into the Combined Code in December 1998 and, in 1999, the Turnbull Report provided directors with additional guidance on how to tackle internal control.

The OECD Principles of Corporate Governance were also published in 1999, but it wasn't until after the Enron and WorldCom debacles and the U.S. Sarbanes-Oxley (SOX) response in 2002 that most other OECD countries made a determined effort to adopt codes of corporate governance. With the exception of the United States, though, individual OECD countries have all adopted corporate governance codes that work on the "comply or explain" principle. The Sarbanes-Oxley Act works on the basis of "comply or be punished." One of the impacts of SOX is that companies that are directly affected by it are requiring their partners and suppliers to certify conformance to SOX, because that gives them greater certainty of ongoing compliance themselves.

At the same time, convergence in accounting and auditing standards across the OECD, and particularly between the United States and the European Union, which contain the vast bulk of the world's capital markets, is driving institutional shareholders to a common framework of governance requirements. Internationally, banks also operate within a common governance and risk management framework defined by the Bank for International Settlements (BIS) and Basel II.[7]

The requirement for all organizations to adopt best corporate governance practices, irrespective of their nationality or location, is—in spite of the resistance of many executives in many jurisdictions—growing stronger. The entry price for access to Western capital markets is, increasingly, acceptance of Western accounting and corporate governance norms. These requirements cannot be met without an effective IT governance framework.

11.6 STRATEGIC AND OPERATIONAL RISK MANAGEMENT

Risk management has always been a key governance issue. The board's job is strategy, and therefore strategic risk has always been a board responsibility. The modern corporation's fundamental goal is to continuously create and add value to its business. That means that strategic management is about finding an appropriate balance between profit maximization and risk reduction.

Strategic risk is the enterprise-level risk of a negative impact on earnings or capital arising from an organization's future business plans and strategies, improper implementation of decisions, or lack of responsiveness to industry changes. It includes risks associated with plans for entering new businesses; expanding existing services; mergers, acquisitions, and divestments; and enhancing the infrastructure. As discussed earlier, information and the technology on which it is stored and with which it is manipulated and communicated is at the heart of twenty-first century business strategy.

Two key strategic risks related to information and communications technology are:

1. Interruptions to business processes and customer services
2. Overspending on IT, placing the company at a cost disadvantage to its competitors

Both these risks should be dealt with as part of the board's strategic risk management process.

In the past few years, the parallel importance of operational risk ("the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events"[8]) has been recognized. The UK's Combined Code requires listed companies to annually review "all material controls, including financial, operational, and compliance controls, and risk management systems."[9] The Turnbull Guidance explicitly requires boards, on *an ongoing basis*, to identify, assess, and deal with significant risks in all areas, including in *information and communications processes.*[10] Sarbanes-Oxley

requires U.S. listed companies (and, increasingly, there is a knock-through effect on their major suppliers) to annually assess the effectiveness of their internal controls, and places a number of other significant governance burdens on executive officers, including the Section 409 requirement that companies notify the Securities and Exchange Commission (SEC) "on a rapid and current basis such additional information concerning material changes in the financial condition or *operations* of the issuer."

Risk assessment has, over the past few years, become a pervasive and invasive concept: A risk assessment must be structured and formal, and nowadays one is expected in almost every context—from a school outing through to a major corporate acquisition. It is certainly a cornerstone of today's corporate governance regimes. In the context of both strategic and operational risk, a risk assessment is the first step that a board can take to controlling the risk; the most important step is the development of a risk treatment plan (in which risks are accepted, controlled, eliminated, or contracted out) that is appropriate in the context of the company's strategic objectives.

11.7 REGULATORY COMPLIANCE

Information is increasingly subject to legislation. Customers, staff, suppliers, tribunals, and law courts all expect organizations to proactively comply with it. There is international, foreign, and industry specific legislation and regulation. All OECD countries have some form of data protection and privacy legislation, and national regulations often overlap, are sometimes contradictory, and almost always lack implementation guidance or adequate precision. Copyright, digital rights, computer misuse, and electronic trading legislation are changing rapidly, and money laundering, proceeds of crime, human rights, and freedom of information legislation all add to the confusion. The Payment Card Industry (PCI) Standard and the Federal Financial Institutions Examination Council (FFIEC) create additional challenges for banks and payment processors.

Complex organizations, with diversified or (partially) virtual business models, operating in and across a number of legal jurisdictions, have an even more complex task. Whereas any one regulation (and its related compliance failure) might apply only to a subsidiary national entity, it is the global parent whose reputation is damaged, and the more failures, the more damage.

While fines and the personal liability of directors and officers can appear as significant risks in relation to some—but not all—of this legislation, few of the regulatory bodies have the resources and capability to proactively investigate and pursue possible transgressors. That will change, and soon.

The need for regulatory compliance should not be allowed to disable the organization; nor should it be ignored. Shareholders do not expect their companies to be in breach of national or international regulations.

Information technology has a key role to play in delivering compliance, but it can do so only if the board has first identified, risk-assessed, prioritized, and

determined resources for a compliance plan across all the jurisdictions in which the organization has exposures.

11.8 INFORMATION RISK

Organizational information is an asset, and therefore, by definition, someone outside the organization wants it. If no one else wanted it, it wouldn't be an asset. Information, to be useful to an organization, must be available (to those who need to use it); it must be confidential (so that competitors can't steal a march); and its integrity must be guaranteed (so that it can be relied upon). Information risk arises from the threats—originating both externally and internally—to the availability, confidentiality, and integrity of the organization's information assets.

Headline figures dramatically illustrate the cost of security failures: the UK's National High Tech Crime Unit (NHTCU) reported[11] that 89 percent of firms interviewed had suffered some form of computer crime in the previous 12 months (up from 83 percent in the previous year), at a cost of at least £2.4 billion.

Threats to information security are wide-ranging, complex, and costly. External threats include casual criminals (virus writers, hackers), organized crime (virus writers, hackers, spammers, fraudsters, industrial spies, ex-employees) and terrorists (including anarchists). More information security incidents (involving members of staff, contractors, and consultants acting either maliciously or carelessly) originate inside the organization than outside it. Barings, Enron, WorldCom, and Arthur Andersen were all bought down by insiders. The indirect costs of these incidents usually far exceed their direct ones, and the reputational impacts are usually even greater. As a result, information security is a fundamental component of the organization's IT governance posture, and its information security solutions must be proportionate to the value at risk and be in line with its strategic and operational goals. These are board decisions, and should not be left to the IT department alone.

11.9 STRATEGIC SYSTEM DEPLOYMENT AND PROJECT GOVERNANCE

Clearly, in today's ICT-enabled business world, organizations are continuously upgrading their existing systems or deploying new systems to improve customer service, reduce cost, improve product or service quality, and deliver new products, services, and business models. These system deployments often involve strategic risk for the organization; they always involve operational risk. Risk management is a board responsibility, and therefore project governance—from inception through to deployment—must also be a board responsibility.

But IT projects are not always delivered successfully. Authoritative research shows that the majority of projects fail to deliver the benefits that justified commencing the project and that, of those that do, the majority come in late and/or over budget. Organizations whose IT projects failed all deployed recognizable project management methodologies; the reasons for failure were invariably to do with failures of project governance rather than simply of operational management.

Increasingly, shareholders are concerned about project failure. In the past, investment analysts were reluctant to assess IT. As they recognize the impact that technology has on business performance (and, consequently, on shareholder value), so they look increasingly for a framework that ensures that IT projects are aligned with commercial objectives and that enables companies to quantify and report in a consistent manner on IT investments.[12]

IT investment decisions (for or against) expose an organization to significant risk—strategic, financial, operational, and competitive. The pace of change is a significant. Project risks must be assessed within the organization's strategic planning and risk management framework for the right decision, one that enhances competitive advantage and delivers measurable value, to be made. Critically, projects need continual oversight; the assumptions on which they were predicated need continual reassessment, and the expected benefits need regular reappraisal. A paranoid, proactive expectation of project failure is the only healthy way of giving it half a chance of success.

Effective IT project governance, therefore, always involves independent, informed, critical board oversight of the implementation of a project that is initiated only after a systematic strategic decision-making process.

11.10 IT GOVERNANCE FRAMEWORKS AND TOOLS

There are a number of formal frameworks that are identified in any survey of IT governance frameworks. An organization that adopts and pursues an IT governance framework must ensure it satisfies four separate audiences: customers, stakeholders, regulators, and the board members themselves.

1. Customers need some certainty that their supplier will be around for the long term, that their personal or business details won't be exposed, and that they will actually get what they're paying for—whether it's quality, services, or goods.
2. Stakeholders (including shareholders, employees, and suppliers) also want to be sure that the organization will be around for the long term, and that their investment (of shareholder cash, uncompensated labor, or as-yet-unpaid invoices) is not only safe but likely to turn into something a (little) better—through effective leveraging of IT and intellectual assets combined with clear-sighted, transparent management and control of the ICT infrastructure within the context of the business model and business strategy.
3. Regulators want to be convinced that their regulations are—and will continue to be—applied.
4. The board members want to be sure that their reputations will survive their time at the organization and that a personal contribution to the settlement of a class action—let alone jail time—will never become an issue for them.

The board's IT governance framework must, in other words, meet the requirements of the regulators, be capable of audit so as to prove to customers and

other stakeholders that the organization is doing things right, and actually work. Regulatory compliance, auditable external certifications, and cost-effective, working solutions are the high-level requirements of any IT governance framework.

11.11 FRAMEWORKS

The most widely recognized frameworks that are usually included in any discussion of formal, third-party IT governance frameworks are:

- Control Objectives for Information and Related Technology (CobiT) is "increasingly internationally accepted as good practice for control over information, IT, and related risks. Its guidance enables an enterprise to implement effective governance over IT."[13]
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission is an integrated framework for internal control.
- ISO 17799:2005 is the international code of best practice for information security, and ISO 27001:2005 is the standard against which an organization's information security management system can be certified as conforming.
- Information Technology Infrastructure Library (ITIL) is an integrated set of best practice recommendations for IT management. ISO 20000 is the world's first standard for IT service management, and it is heavily based on ITIL.
- There are also project management methodologies, such as the UK's Prince2™ and the Project Management Institute's PMBoK® and OPM3®.

While each of these frameworks is often described as an IT governance framework, none of them actually provides a comprehensive IT governance framework that fully recognizes the crucial role of the board in governing IT or that meets the requirements outlined earlier; they do each have different strengths and weaknesses, and there are overlaps between them. Components of each can usefully be deployed as part of an integrated and comprehensive framework.

ITGI, the owners of CobiT, and the OGC, owners of ITIL, have already attempted a clause-to-clause mapping between these two frameworks and ISO 17799.[14]

11.12 AS 8015-2005

The one formal IT governance framework that does recognize the essential nature of the board's role is AS 8015-2005, the Australian standard for the corporate governance of information and communication technology.[15]

The standard lays out six simple principles for "good corporate governance of IT":

1. Establish clearly understood responsibilities.
2. Plan ICT to support the organization.
3. Acquire ICT validly.

4. Ensure that ICT performs well whenever required.
5. Ensure ICT conforms with formal rules.
6. Ensure ICT respects human factors.

It is equally clear that the directors should govern ICT through three main tasks:

1. Evaluate the use of ICT.
2. Direct preparation and implementation of plans and policies.
3. Monitor conformance to policies and performance against plans.

The standard then provides a single model for IT governance and the evaluate-direct-monitor cycle, which is shown in Exhibit 11.1.

The detail of the standard then describes, for each of the six principles, the more detailed actions that the directors have to take in the evaluate-direct-monitor cycle to implement the principle.

While AS 8015-2005 is valuable in that it provides a practical and workable IT governance framework, it doesn't deal with the operational project governance or information security issues faced by the organization, nor does it contain a detailed enterprise risk assessment model.

11.13 IT GOVERNANCE—THE IMPLEMENTATION CHALLENGE

It is important to recognize that there are no silver bullets for the implementation of IT governance. IT governance dashboards, for instance, are a useful tool for monitoring activity; they are, however, useful only once an organization has decided what it wants to monitor—and why.

An IT governance framework has to suit the requirements of the organization that is implementing it. It can sometimes appear to the busy executive that there are as many competing IT governance frameworks and tools as there are regulations and business requirements. What is needed is a framework of frameworks that enables organizations to identify how all these frameworks and methodologies relate to one another, and how they might be used together to best advantage.

The Calder-Moir Framework[16] has been developed to do precisely that. It recognizes that most organizations will wish to cherry-pick specific guidance that suits their specific business needs. It is a freely available resource that identifies how all the frameworks and methodologies described in this chapter fit together, and that also describes the role of other, equally relevant frameworks such as the Zachman IT architecture framework and the Baldrige quality criteria.

11.14 BENEFITS OF AN IT GOVERNANCE FRAMEWORK

Good governance makes sense. In 1996, McKinsey and Company found that two-thirds of the companies in a survey would pay an 11 percent premium for the stock of a company with good governance practices.[17] More than that, "companies whose boards engage in one or more of [the] three governance practices

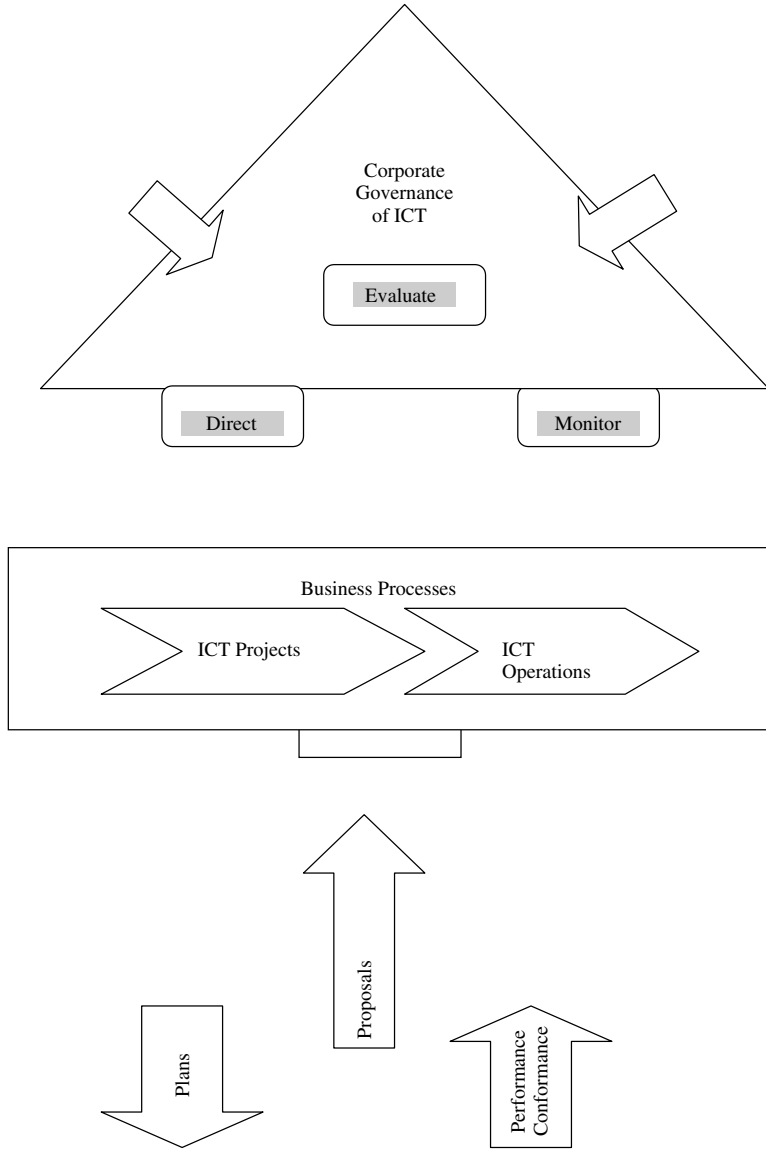


EXHIBIT 11.1 AS 8015-2005: MODEL FOR CORPORATE GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY

that signal board independence from management outperform their peers and produce higher returns for their shareholders,"[18] as measured by economic value added (EVA)—earnings (posttax) in excess of the cost of the capital required to generate them.

And if good governance makes sense, good IT governance makes even more sense: "Top-performing firms succeed where others fail by implementing

effective IT governance to support their strategies. Firms with above-average IT governance following a specific strategy ... had more than 20 percent higher profits than firms with poor governance following the same strategy."[19] Research by Weill and Ross also indicates that "top-performing enterprises generate returns on their investments up to 40 percent greater than their competitors."[20]

Notes

1. Eliot Spitzer, interviewed in the *Wall Street Journal,* April 8, 2005.
2. *OECD Principles of Corporate Governance,* 1999.
3. Alan Calder, "IT Governance: Guidelines for Directors," ITGP, 2005.
4. The World Economic Forum web site at www.weforum.org/gitr has the full report and the comparative 2004 and 2003 rankings.
5. The term *business model* "seems to refer to a loose conception of how a company does business and generates revenue. Yet simply having a business model is an exceedingly low bar to set for building a company. Generating revenue is a far cry from creating economic value, and no business model can be evaluated independently of industry structure. The business model approach to management becomes an invitation for faulty thinking and self-delusion." Michael E. Porter, "Strategy and the Internet," *Harvard Business Review,* March 2001.
6. See Gary Hamel, *Leading the Revolution* (Boston: Harvard Business School Press, 2000).
7. "International Convergence of Capital Measurement and Capital Standards: A Revised Framework" was published by the Basel Committee on Banking Supervision in June 2004.
8. "Operational Risk," a consultative document from the Basel Committee on Banking Supervision in January 2001.
9. Combined Code on Corporate Governance, Section C.2.1, July 2003.
10. Turnbull Guidance, paragraph 21.
11. "Hi-Tech Crime: The Impact on UK Business 2005," survey conducted by NOP for the UK's NHTCU.
12. HP IT Governance Roundtable, October 24, 2002.
13. www.isaca.org.
14. Copies are available from the web sites of both those organizations and from www .itgovernance.co.uk/page.it_governance.
15. SAI Global, at www.standards.com.au.
16. www.itgovernance.co.uk/page.framework.
17. Ned Regan in "Entrepreneurial Companies, Strong Boards and Shareholder Value," *Corporate Board Member* magazine, August 2002.
18. Ira M. Millstein ad Paul W. MacAvoy, "The Active Board of Directors and Improved Performance of the Large Publicly Traded Corporation," *Columbia Law Review* 98 (5) (June 1998): 1283–1322.
19. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Weill and Ross, Boston: HBS Press, 2004.
20. Ibid.

CHAPTER 12

ISO 27001 AND ISO 17799

Alan Calder

12.1 ISO 27001 AND ISO 17799—THE INFORMATION SECURITY STANDARDS

The replacement, in late 2005, of BS 77799-2:2002 by the international information security management system (ISMS) standard ISO/IEC 27001:2005 marks the coming of age of information security management. ISO 27001 is the international standard for information security management systems, and it provides organizations with best practice guidance for identifying, assessing, and controlling information risks in strategic business plans and everyday operational environments. It's *the* essential standard for the information age organization. It has an important and symbiotic relationship with another international standard, ISO/IEC 17799:2005, which is discussed later in this chapter.

(a) BACKGROUND TO ISO 27001. In the first eight years that BS 7799 existed as a standard against which organizations could gain an external certification, about 1,000 were successful, worldwide. This number doubled in the subsequent

12 months. With the internationalization of BS 7799, that number will grow geometrically. This chapter looks at why organizations are increasingly turning to this information security management standard.

According to an Information Security Ltd survey, by far the most common drivers for organizations that have, historically, been successful in achieving BS 7799 "were commercial: to increase the confidence of customers, or possibly to encourage suppliers, when dealing with the organization."[1] For others, according to the same survey, an information security management standard is "becoming an increasing requirement in tender documents, as well as contracts"; for a very sizable minority, gaining a competitive advantage over their competitors has been equally important.

Technology—specifically information technology—is transforming the economic and social worlds in which we work, play, and live. Whether or not this is a good thing is irrelevant. The fact is that, for most people, information was stored, 20 years ago, on pieces of paper. Small numbers of large mainframe computers batch-processed mundane transactions, and a credit card application could take several weeks. Corporations wrote their own computer programs and avoiding GIGO (garbage in, garbage out) was the head of IT's prime objective. Fax machines were transforming a business communication infrastructure that still depended on expensive fixed telephone lines. Information, when it existed, was hard to lay your hands on and even harder to use, manipulate, or transform.

Today, information overload is a commonplace complaint. Computers are ubiquitous, communication can be globally instantaneous, and someone else can get a credit card in your name in a matter of minutes.

As we've shifted from a manufacturing to an information economy, the structure of organizational value has changed dramatically. The intangible assets (mostly intellectual capital) of most Organization for Economic Cooperation and Development (OECD) organizations are now worth substantially more than their tangible assets, and this trend is unlikely to reverse.

Information is the lifeblood of the modern business. All organizations possess and use critical or sensitive information. Roughly nine-tenths of businesses now send e-mail across the Internet, browse the Web, and have a web site; and 87 percent of them now identify themselves as highly dependent on electronic information and the systems that process it. Information and information systems are at the heart of any organization trying to operate in the high-speed wired world of the twenty-first century.

Business rewards come from taking risks—managed, controlled risk taking, but risk taking nonetheless. The business environment has always been full of threats, from employees and competitors through criminals and corporate spies to governments and the external environment. The change in the structure of business value has led to a transformation in the business threat environment.

The proliferation of increasingly complex, sophisticated, and global threats to this information and its systems, in combination with the compliance requirements of a flood of computer- and privacy-related regulation around the world, is forcing organizations to take a more joined-up view of information security. Hardware-, software-, and vendor-driven solutions to individual information security challenges no longer cut the mustard. On their own, in fact, they are dangerously inadequate.

News headlines about hackers, viruses, and online fraud are just the public tip of the data insecurity iceberg. Business losses through computer failure, major interruption to data and operating systems, and the theft or loss of intellectual property or key business data are more significant and more expensive.

Organizations face criminal damages, reputation loss, and business failure if they omit to adequately secure their information. Directors face loss of personal reputation and jail time if they fail in their duty to protect the information their organizations are holding.

But computer security technology, on its own, simply does not protect information. On its own, it just wastes money, gives a false sense of security, and decreases business efficiency. What organizations need is a structured method for identifying the real information risks they face, the financial impact of those threats, and appropriate methods of mitigating those specific, identified risks. Securing information is not rocket science, whatever the technology vendors might say. Information is at risk as much through human behavior (and inattention) as it is through anything else. Securing information therefore requires an approach that is as much about process and individual behavior as it is about technological defenses.

And no organization has either the time or the resources to try to work out, on its own and from first principles, how to do this effectively. Apart from anything else, the time and error profile is likely to be unattractive.

No organization needs to try to do so. ISO 27001 already exists. This standard, which contains current information security international best practice that has already been successfully implemented in more than 2,000 organizations around the world, gives organizations a reliable and effective framework for deploying an information security management system that will preserve its assets, protect its directors, and improve its competitiveness.

(b) INFORMATION SECURITY STANDARDS ORIGINATING BODY. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) established a joint technical committee, ISO/IEC JTC 1, to deal with their mutual interest in the field of information technology. This committee has a number of subcommittees, and one of these, SC 27, is responsible for IT security techniques. This committee (ISO/IEC JTC 1/SC 27) is responsible for producing both current and future international information security standards.

(c) ISO/IEC 27001:2005 (ISO 27001). This is the most recent, most up-to-date international version of a standard specification for an information security management system. It is vendor-neutral and technology-independent. It is designed for use in organizations of all sizes ("intended to be applicable to all organizations, regardless of type, size, and nature"[2]) and in every sector (e.g., "commercial enterprises, government agencies, not-for-profit organizations")[3] anywhere in the world.

It is a management system, not a technology specification, and this is reflected in its formal title, which is "Information Technology—Security Techniques—Information Security Management Systems—Requirements." ISO 27001 is also the first of a series of international information security standards, all of which will have ISO 27000 numbers.

It is a specification. It uses words like *shall*. It sets out requirements. It can therefore "be used to assess conformance by interested internal and external parties." It is, in other words, the specific document against which an ISMS can be assessed, and it provides a basis for assessments that can be carried out by first, second, or third parties. A third-party assessment, when carried out by an accredited certification body, can lead to the award of an accredited certificate of conformity to the standard. Such a certificate has an international status.

(d) ISO/IEC 17799:2005 (ISO 17799). This standard is titled "Information Technology—Security Techniques—Code of Practice for Information Security Management." Published in July 2005, it replaced ISO/IEC 17799:2000, which has been withdrawn. During 2007, this Code of Practice is expected to be renumbered as ISO/IEC 27002.

It is important to note that ISO 17799 is a Code of Practice, not a specification. A Code of Practice is a set of guidelines that use words like *should* and *may*. In other words, it allows individual organizations to choose which elements of the standard to implement, and which not. A specification, such as ISO 27001, does not provide any such latitude.

ISO 17799 was developed originally as a Code of Practice in order to provide a framework for international best practice in information security management and systems interoperability. While it provided guidance, primarily around the implementation of specific information security controls, it provided no guidance of any sort for the development and deployment of the management system within which those controls might be appropriate.

12.2 ISO 17799 VERSUS ISO 27001

ISO 17799, in other words, does not provide the basis for an international certification scheme. Only ISO 27001 does that.

(a) CORRESPONDENCE BETWEEN THE TWO STANDARDS. The relationship between the two standards is, however, symbiotic. Annex A to ISO/IEC 27001:

2005 lists the 133 controls that are in ISO/IEC 17799:2005 follows the same numbering system and uses the same words for those controls. The preface to ISO 27001 states that "the control objectives and controls referred to in this edition are directly derived from and aligned with those listed in ISO/IEC 17799:2005." ISO/IEC 27001 requires that "control objectives and controls from Annex A shall be selected" in order to meet the "requirements identified by the risk assessment and risk treatment process."

ISO 17799 also provides substantial implementation guidance on how individual controls should be approached. Anyone implementing an ISO 27001 ISMS will therefore need to acquire and study copies of *both* ISO 27001 and ISO 17799.

While ISO 27001 mandates the use of ISO 17799 as a source of guidance on controls, control selection, and control implementation, it does not limit the organization's choice of controls. In fact, the preface goes on to state that "the list of control objectives and controls in this ISO Standard is not exhaustive and an organization might consider that additional control objectives and controls are necessary."[4]

(b) INTEGRATION OF MANAGEMENT SYSTEMS. Organizations increasingly seek certification against more than one international standard, such as ISO 9001 and ISO 14001. They also look to deploy best practices from a number of sources, such as Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (CobiT), and ISO 20000. ISO 27001 provides guidance on integration with other ISO standards.

Annex C to ISO 27001 (which is informative, not mandatory; in other words, no organization is required to try to integrate its management systems) shows how its individual clauses of ISO 27001 correspond to the clauses of ISO 9001:2000 and ISO 14001:2004. For most, but not all, organizations, the critical correspondences will be between ISO 27001 and ISO 9001. The following ISO 27001 clauses are the starting points for management system integration:

- Clause 4.3, which deals with documentation requirements.
- Clause 5.1, which deals with management commitment.
- Clause 7, which deals with management review.
- Clause 6, which deals with internal audits.

These clauses, between them, make possible the deployment of common documentation, management, and audit processes for both management systems.

The definitions used in both information security standards are also intended to be consistent with one another and to be consistent with those used in related information security standards, such as ISO/IEC Guide 73:2002, ISO/IEC 13335-1:2004, and so on.

(c) IT GOVERNANCE AND INFORMATION SECURITY MANAGEMENT. While IT governance is the discipline that deals with the structures, standards, and processes that boards and management teams apply to effectively manage, protect,

and exploit their organization's information assets, information security management is that subset of IT governance that focuses on protecting and securing the organization's information assets.

(d) RISKS TO INFORMATION ASSETS. Information assets (and *asset* is defined in ISO 27001 as "anything that has value to an organization") are subject to a wide range of threats, both external and internal, ranging from the random to the highly specific. Risks include acts of nature, fraud and other criminal activity, user error, and system failure. Information risks can impact one or more of the three fundamental attributes of an information asset: its availability, its confidentiality, and/or its integrity.

These three attributes are defined in ISO 27001:

1. *Availability:* "the property of being accessible and usable upon demand by an authorized entity," which allows for the possibility that information has to be accessed by software programs as well as human users.
2. *Confidentiality:* "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes."
3. *Integrity:* "the property of safeguarding the accuracy and completeness of assets."

(e) INFORMATION SECURITY. ISO 27001 therefore defines information security as the "preservation of confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, nonrepudiation, and reliability can also be involved."

(f) INFORMATION SECURITY MANAGEMENT SYSTEM. ISO 27001 defines an information security management system (ISMS) as "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources." An ISMS, in other words, exists to preserve confidentiality, integrity, and availability.

(g) ISO 27001 AS A MODEL FOR THE ISMS. In the simple terms of the standard, it is a useful model for "establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS."[5] It is a model that can be applied anywhere in the world and understood anywhere in the world. It is consistent and coherent; it contains the assembled best practice, experience, and expertise gathered from implementations throughout the world over the past 10 years; and it is technology-neutral. It is designed for implementation in any hardware or software environment.

It should be noted that having an ISO 27001-compliant ISMS will not automatically "in itself confer immunity from legal obligations."[6] In other words,

the organization will have to ensure that it understands the range of legislation and regulation with which it must comply, and ensure that these requirements are reflected in its ISMS.

(h) LEGAL AND REGULATORY FRAMEWORK. The legal and regulatory framework (see clause 4.2.1. b.2 of ISO 27001) creates a specific perspective on the scoping of the ISMS for all organizations. Clearly, information and information management processes that are all within the scope of any single regulation or other legal requirement must also all be within the scope of the ISMS.

(i) PROCESS APPROACH AND THE PDCA CYCLE. ISO 27001 mandates the use of a plan-do-check-act (PDCA) approach for the development and deployment of the ISMS. This approach, widely known as the plan-do-check-act (PDCA) model, will be familiar to quality and business managers everywhere.

The PDCA model or cycle was originated in the 1950s by W. Edwards Deming. It says that business processes should be treated as though they are in a continuous feedback loop so that managers can identify and change those parts of the process that need improvement. The process, or an improvement to the process, should first be planned, then implemented and its performance measured; then the measurements should be checked against the planned specification and any deviations or potential improvements should be identified and, finally, reported to management for a decision about what action to take.

Application of the PDCA cycle to a process approach means that, following the basic principles of process design, there must be both inputs to and outputs from the process. An ISMS takes as its input "the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meet those requirements and expectations."[7]

This means is that the PDCA model is applied at two levels: at the strategic level, in terms of the overall development of the ISMS itself, and at the tactical level, in terms of the development of each of the processes within the ISMS. There is, therefore, an important linkage between each of the clauses of the PDCA model and the clauses of the standard.

(j) ESTABLISHING THE ISMS. The standard describes how to design and implement an ISMS. The most important clause is the one that has the most bearing on the effectiveness or otherwise of the ISMS: clause 4.2.1 on establishing the ISMS.

Clause 4.2.1 deals with six critical items:

1. *Scope:* the definition of the organization to which the ISMS applies.
2. *Policy:* the board's information security policy, which sets the guidelines for the whole ISMS.
3. *Asset inventory:* the information assets of all types (tangible and intangible) that are to be the subject of the ISMS.

4. *Risk assessment:* the identification of the risks that relate to each asset.
5. *Risk treatment plan:* the identification of how each risk is to be dealt with, within the context of the board's overall approach to risk.
6. *Statement of Applicability:* the description of which of the controls in Annex A of ISO 27001 have been applied, and how, and which have not been applied, together with a justification for their exclusion.

Of course, designing, implementing, and auditing the controls are what most people think information security is all about. In fact, the control design and implementation stage is really only the outcome of the more critical, business-focused stages of the process, which are those that enable the organization to determine what the appropriate controls might be.

(k) POLICY AND BUSINESS OBJECTIVES. While scoping is a critical first stage in getting a workable ISMS, it is even more important to recognize how corporate information security policy should drive the ISMS. The standard requires a formal policy document that sets a "clear policy direction in line with business objectives." The standard's perspective is that a successful and useful ISMS will be one that does not undermine or block business activity. The significant risk in implementing systems that block business activity, that are not (in the language of the standard) in line with business objectives, is that people inside the business will ignore or bypass the ISMS controls.

So, the information security policy is important, and it must be drafted so that every word in it is clear, unambiguous, and meaningful (providing a "clear direction"). Finalization of the policy is dependent on the completion of the scoping of the project. Scoping, one of the nine keys[8] to a successful ISO 27001 implementation, makes an essential contribution to the policy definition.

The information security policy must be signed off on by the board and made available as appropriate to anyone who needs it.

(l) RISK ASSESSMENT. The most important step in determining what might be the critical controls is the risk assessment. Of course, all organizations face risks of one sort or another on a daily basis, and, today, a substantial part of the corporate governance agenda revolves around the expectation that boards of directors will take appropriate steps to identify and control risks to the enterprise of which they are custodians. Enterprise Risk Management (ERM) is increasingly recognized as a key discipline for all organizations.

Risk management is a discipline that exists to deal with nonspeculative risks, which are those risks from which only a loss can occur. In other words, speculative risks, those from which *either* a profit *or* a loss can occur, can be seen as the subject of the organization's business strategy, whereas nonspeculative risks, those that can reduce the value of the assets with which the organization undertakes its speculative business activity, are (usually) the subject of what the standard calls a "risk treatment plan." These nonspeculative risks, because they

can be identified and plans made to deal with them ahead of their occurrence, are sometimes called permanent and pure risks, in order to differentiate them from the crisis and speculative types.

Risk treatment plans have four linked objectives. These are to (1) eliminate risks, (2) reduce those that can't be eliminated to "acceptable" levels, and then to either (3) live with them, exercising carefully the controls that keep them "acceptable," or (4) transfer them, by means of insurance, to some other organization.

The definition of what is "acceptable" is therefore critical to any risk treatment plan, and the standard requires management (in clause 5.1.f) to "decide the criteria for accepting risks and for acceptable risk levels." Note that this is a management requirement, and a process must therefore be adopted by management to make these decisions, which ensures that the decisions made in respect to information security risk fit "within the context of the organization's overall business activities and the risks they face."[9]

This is the second area in which the two standards are directly complementary. Whereas ISO 27001 specifies the risk assessment steps that must be followed, ISO 17799:2005 provides substantial further guidance on the risk assessment but deliberately does not provide detailed guidance on how the assessment is to be conducted. This is because every organization is encouraged to choose the approach that is most applicable for its industry, complexity, and risk environment.

A risk treatment plan can only be drawn up once the risks have been identified, analyzed, and assessed. Risk analysis is a subjective exercise in any environment where returns are derived from taking risks. Risk assessment is based on a data-gathering process and, as all individual inputs into the analysis will reflect individual prejudice, so the process of information gathering should question inputs to establish what really is known—and what unknown. The risk assessment process must follow the specific requirements of the standard; this part of the project is enormously time and resource consuming and can be carried through only by deploying a risk assessment tool that is specifically designed to support an ISO 27001 risk assessment.

Qualitative risk assessment is by far the most widely used approach to risk analysis and is the approach expected by clause 4.2.1.d (identify the risks) of the standard. Numeric probability data is not required, and only estimated potential total loss can be used. Most qualitative risk analysis methodologies make use of a number of interrelated elements, and they are best laid out in tabular form in a corporate asset and risk log, so that, for each asset, its owner(s), threat(s), vulnerability(ies), and impact(s) are identified.

The standard sets out six steps that must be followed in carrying out a risk assessment:

1. Identify the assets within the scope of the ISMS.
2. Identify threats to the confidentiality, availability, and integrity of those assets.

3. Identify the vulnerabilities those threats could exploit.
4. Assess the possible impacts of those threats.
5. Assess the likelihood of those events occurring.
6. Evaluate the risk.

While there are a number of similarities between an ISO 27001 risk assessment and any other that might be required, remember that the ISO 27001 risk assessment has to be conducted in a certain way. The standard itself describes how this should be done, as does BS 7799-3:2006; there are also now some books that accurately and correctly describe this process.

(m) RISK TREATMENT PLAN. The risk assessment process must be formally defined and described, and the responsibility for carrying it out, reviewing it, and renewing it must be formally allocated. At the heart of this plan is a detailed schedule, which shows, for each identified risk, how the organization has decided to treat it, what controls are already in place, what additional controls are considered necessary, and the time frame for implementing them. The acceptable level of risk needs to be identified for each risk, as well as the risk treatment option that will bring the risk within an acceptable level.

The risk treatment plan links the risk assessment (detailed, as described in the previous chapter, in the corporate information asset and risk log) to the identification and design of appropriate controls, as described in the Statement of Applicability, such that the board-defined approach to risk is implemented, tested, and improved. This plan should also ensure that there is adequate funding and resources for implementation of the selected controls and should set out clearly what these are.

The risk treatment plan should also identify the individual competence and broader training and awareness requirements necessary for its execution and continuous improvement.

The risk treatment plan is, in other words, the key document that links all four phases of the PDCA cycle for the ISMS. It is a high-level, documented identification of who is responsible for delivering which risk management objectives, of how this is to be done, with what resources, and how this is to be assessed and improved. At its core, it is the detailed schedule describing who is responsible for taking what action, in respect to each risk, to bring it within board-defined acceptable levels.

12.3 CONCLUSION

It should by now be clear that an ISMS developed in line with the ISO 27001 specification will be one that focuses on business objectives and identifies controls that are appropriate to clearly identified and evaluated risks to individual information assets.

An effective ISMS will also be one that is integrated into the overall management system of the enterprise, delivers meaningful compliance with the full

range of information security regulation to which the organization is subject, and, most important, provides real security against the full range of information security risks faced in the marketplace.

12.4 ESSENTIAL FURTHER READING

The standards themselves are available from all national standards institutes and from www.itgovernance.co.uk/page.standards.

The following works are by Alan Calder.

Implementing ISO 27001 and ISO 17799: A Management Guide (van Haren, 2006)
International IT Governance: An Executive Guide to ISO 27001/ISO 17799 (Kogan Page, 2006)
ISO 27001 and ISO 17799: A Management Guide (van Haren, 2006)
Nine Steps to Success: An ISO 27001 Implementation Overview (ITGP, 2005)
The Case for ISO 27001 (ITGP, 2005)

Notes

1. Information Security, BS7799 Survey 2005—Information Security Ltd.
2. ISO/IEC 27001:2005, Application 1.2
3. ISO/IEC 27001:2005, Scope 1.1.
4. ISO/IEC 27001:2005, Preface.
5. All four quotes are from ISO/IEC 27001:2005, Introduction, General 0.1.
6. ISO/IEC 27001:2005, Title Note.
7. Ibid.
8. Alan Calder, *Nine Keys to Success: an ISO 27001 Implementation Overview* (ITG Publishing, 2005).
9. ISO/IEC 27001:2005 4.1, General Requirements.

CHAPTER 13

COBIT

Richard Marti

13.1 BACKGROUND

Control Objectives for Information and Related Technology (COBIT) is an IT governance control framework. COBIT's purpose is to ensure IT resources are aligned with an enterprise's business objectives so that services delivered balance IT risks and returns. COBIT defines 34 significant processes, links 318 detailed controls activities to them, and defines an internal control framework for all of them.

COBIT is designed for three distinct audiences:

1. *Management*—to help them to balance risk and control investment in an often unpredictable IT environment
2. *Users*—to obtain assurance on the security and controls of IT services
3. *Information systems auditors*—to substantiate their opinions and/or to provide better advice to management on internal controls

13.2 HISTORY

The CobiT framework was defined in the first edition, published in 1996. Research for second edition (released in 1998) included the collection and analysis of identified international sources and was carried out by teams in:

- Europe (Free University of Amsterdam, the Netherlands)
- United States (California Polytechnic University)
- Australia (University of New South Wales)

The CobiT third edition project (released in 2000) consisted of developing the management guidelines and updating the second edition based on new and revised international references. In late 2005, the Information Technology Governance Institute (ITGI) released CobiT 4.x.

CobiT Evolution Summary

- 1994 CobiT first edition—Audit
- 1998 CobiT second edition—Control
- 2000 CobiT third edition—Management
- 2005 CobiT fourth edition—Governance

CobiT's processes and control objectives are segmented into four domains:

1. Planning and Organization (PO)
2. Acquisition and Implementation (AI)
3. Delivery and Support (DS)
4. Monitoring (M)

(a) PLANNING AND ORGANIZATION. Planning and organization includes the overall strategy and tactical details to support an organization and infrastructure that will meet the organization's objectives.

Objective

- Strategy and tactics for IT contribution
- Meeting business objectives
- Appropriately planned, communicated, and managed
- Proper organization and technological infrastructure
- PO1 Define a strategic IT plan
- PO2 Define the information architecture
- PO3 Determine the technological direction
- PO4 Define the IT organization and relationships
- PO5 Manage the IT investment
- PO6 Communicate management aims and directions

- PO7 Manage human resources
- PO8 Ensure compliance with external requirements
- PO9 Assess risks
- PO10 Manage projects
- PO11 Manage quality

(b) ACQUISITION AND IMPLEMENTATION. Acquisition and implementation includes the procurement, development, and maintenance of all identified software applications, databases, infrastructures, and procedures.

OBJECTIVE

- Realization of IT strategy
- Solutions identified, developed or acquired, and implemented
- Solutions integrated into business process
- Change and maintenance of systems
- AI1 Identify automated solutions
- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology infrastructure
- AI4 Develop and maintain IT procedures
- AI5 Install and accredit systems
- AI6 Manage changes

(c) DELIVERY AND SUPPORT. Delivery and support includes all operational activities to meet agreed upon service levels for the organization.

OBJECTIVE

- Actual delivery of required services
- Actual operations through security, including training
- Establishment of support processes
- Actual processing of data by applications
- DS1 Define and manage service levels
- DS2 Manage third-party services
- DS3 Manage performance and capacity
- DS4 Ensure continuous service
- DS5 Ensure system security
- DS6 Identify and allocate cost
- DS7 Educate and train users
- DS8 Assist and advise customers
- DS9 Manage the configuration
- DS10 Manage problems and incidents

- DS11 Manage data
- DS12 Manage facilities
- DS13 Manage operations

(d) MONITORING. Monitoring includes the ongoing activities to assess, measure, benchmark, and audit IT processes.

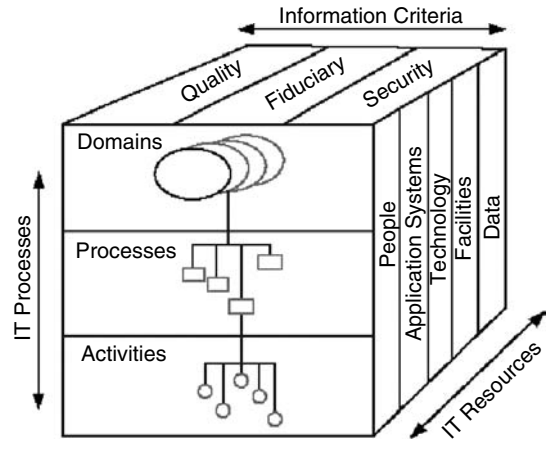
OBJECTIVE

- Regular assessment of all IT processes
- Compliance with and quality of controls
- M1 Monitor the processes
- M2 Assess internal control adequacy
- M3 Obtain independent assurance
- M4 Provide for independent audit

13.3 COBIT CUBE

CobiT offers multidirectional measurement views of IT services broadly divided into three different areas: IT processes (which exist to support business objectives), IT resources (human and capital assets), and information criteria. (See Exhibit 13.1).

(a) CobiT 4.x. CobiT 4.x offers an excellent linkage between business goals and IT goals/processes that was a missing component in the earlier version. Only four



Source: www.itgi.org.

EXHIBIT 13.1 CobiT CUBE

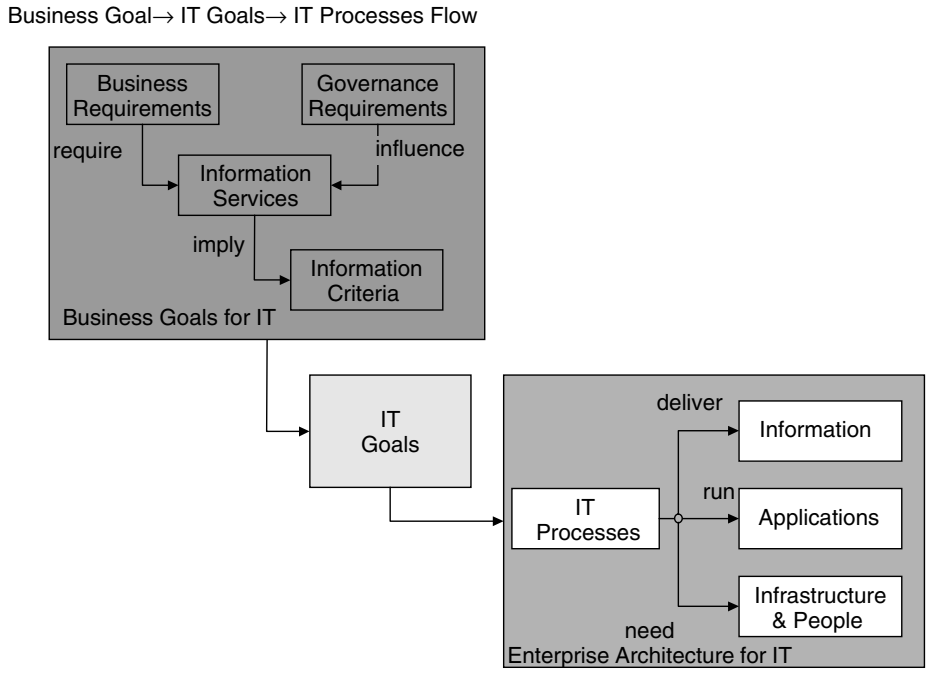


Exhibit 13.2 CobiT 4.x

resources (applications, information, infrastructure, and people), together with IT goals and processes, form a simple enterprise architecture model. Framework, Control Objectives, and Management Guidelines are now one integrated book. (See Exhibit 13.2.)

(b) MAIN CHANGES IN CobiT 4.x

1. There are two new processes (ensure compliance and provide governance).
2. PO has one process less, AI one more (IT procurement).
3. AI5 plus some of AI6 is now AI7—test and release at end of solutions delivery life cycle.
4. DS8 and DS10 are now aligned with Information Technology Infrastructure Library (ITIL).
5. DS11 now strictly addresses only data management.

(c) CobiT 4.x HIGHLIGHTS. CobiT 4.x is an evolution from the third edition based on the same principles and structures—no need to throw away current work. It builds on and extends the third edition with stronger business focus and governance practices.

Full cross-references between processes and control objectives map in both directions, which makes it easy to understand the scope and purpose of a process and makes its ownership clearer.

Metrics link into the mapping of business goals to IT goals to IT processes; they are fewer, more measurable, and have a greater insight-to-effort ratio. The metrics support the cascade of IT, process, and activity goals, providing an integrated system.

- *IT governance*. CobiT 4.x contains a matrix mapping for all IT processes to the governance domains.
- *Business requirements*. Based on extensive research, a table is provided showing the relationship among business goals, IT goals, and CobiT's IT processes to help users identify business-to-IT linkages in their own organizations.
- *Enterprise architecture*. CobiT 4.x provides charts for identifying who is responsible, accountable, consulted, and informed (RACI) to address process roles and responsibilities for each IT process.

(d) CobiT 4.x MATURITY MODEL

1. **Nonexistent.** Complete lack of any recognizable processes.
2. **Initial.** There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
3. **Repeatable.** Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
4. **Defined.** Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.
5. **Managed.** It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
6. **Optimized.** Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with

other enterprises. IT is used in an integrated way to automate the work flow, providing tools to improve quality and effectiveness and making the enterprise quick to adapt.

13.4 LINKING BUSINESS GOALS TO IT GOALS

IT goals must align with business goals to measure IT performance. CobiT 4.x provides an excellent framework to achieve this daunting task. Ideally, IT should run like a business that will provide measurable goals. Business goals can be categorized at high level in four areas:

1. *Financial perspective.* Expand market share, increase revenue and return on investment (ROI), optimize asset utilization, and manage business risks.
2. *Customer perspective.* Improve customer service; offer competitive products and services, nonstop service availability, better time to market, and economical service delivery.
3. *Internal perspective.* Automate and integrate enterprise value chain, improve business process functionality, reduce process costs, comply with external laws and regulations, comply with internal policies, and improve operational productivity.
4. *Growth perspective.* Focus on business innovation, strategic decision making, and employee retention.

(a) BUSINESS REQUIREMENTS MAPPING WITH IT RESOURCES/PROCESSES. Business goals that drive business requirements are measured according to three information criteria: quality, security, and fiduciary.

(i) Quality

- *Effectiveness* deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent, and usable manner.
- *Efficiency* concerns the provision of information through the optimal (most productive and economical) usage of resources.

(ii) Security

- *Confidentiality* concerns protection of sensitive information from unauthorized disclosure.
- *Integrity* relates to the accuracy and completeness of information as well as to its validity in accordance with the business's set of values and expectations.

- *Availability* relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.

(iii) Fiduciary

- *Compliance* deals with complying with those laws, regulations, and contractual arrangements to which the business process is subject (i.e., externally imposed business criteria).
- *Reliability of information* relates to systems providing management with appropriate information for it to use in operating the entity, in providing financial reporting to users of the financial information, and in providing information to report to regulatory bodies with regard to compliance with laws and regulations.

13.5 HOW WILL CobiT 4.x IMPACT/BENEFIT USERS?

CobiT 4.x is an evolution from the third edition; hence current work is usable. It provides improved business orientation and examples to help users define better measures of their own. It is more complete and provides fuller coverage of IT governance. It helps focus on the right areas and enables IT management and auditors to demonstrate how well IT is being governed. It enhances IT process information, business-oriented goals and metrics, and a refined maturity model. It helps users better align IT governance with business drivers and then benchmark and implement process capability and performance. It improves communication with business executives as to IT strategy, business alignment, and IT costs. It makes IT audits easier, as well as security, problem management, and change management.

13.6 CONCLUSION

One of the important business drivers is broad acceptance of CobiT frameworks by external auditors. This makes a relatively easy sale for IT management to convince business executives to agree with the framework that links overall business goals.

- CobiT is an excellent framework for the global IT governance and controls environment.
- It is flexible and mapping with industry-leading frameworks such as ITIL, ISO/IEC 17799, PMBOK, CMMI, and PRINCE2.
- It offers a toolkit for implementing an IT governance and controls environment.

References

www.itgi.org
www.isaca.org

PART 3

OPERATIONAL RISK

CHAPTER 14

OPERATIONAL RISK MANAGEMENT (ORM) BEST PRACTICES

Anthony Tarantino, PhD

14.1 INTRODUCTION

Risk and opportunity go hand in hand—two sides of the same coin. There are risks in all activities, and opportunities always come with inherent risks. It is not possible to completely eliminate risks. The goal is to identify, manage, and mitigate risks, and do so in a cost-effective manner. Operational risk is caused by the failure of internal controls over people, process, technology, and external events. It can include a wide variety of problems: external fraud, internal fraud, inadvertent errors, technology failures, incorrect data entry, natural disasters, regulatory changes, terrorism, and so on.

Interest in operational risk management (ORM) best practices will continue to grow in importance as organizations realize the limitations of the Committee of Sponsoring Organizations (COSO) framework, which lacks a means to measure and quantify risk. The 1992 COSO framework was updated in 2004 with Enterprise Risk Management (ERM), also know as COSO II. ERM would appear on the surface to have addressed operational risk, but falls short in not providing a means to quantify and measure risk. Both COSO I and II provide only a simple pass-fail evaluation of risk. There is no reward for doing better than a mere passing grade. It is also unfortunate that COSO implies that risk is negative. Organizations that are too risk averse will struggle to grow and prosper.

Banking is at the forefront of the effort to quantify and measure operational risk and as such can be a role model beyond the financial services industry. The

Basel II accord requires banks to measure operational risk and requires larger banks to use advanced quantification and qualification techniques to measure, control, and report on operational risk. For all organizations, operational risk management should be seen as a means to improve the quality and stability of earnings and enhance an organization's competitive and reputational position.

The Basel committee has categorized operational risk on a high level, as shown in Exhibit 14.1. What follows are some recommendations to improve operational risk management that are applicable to most larger organizations. Smaller organizations will be able to adopt many of the more basic recommendations as well.

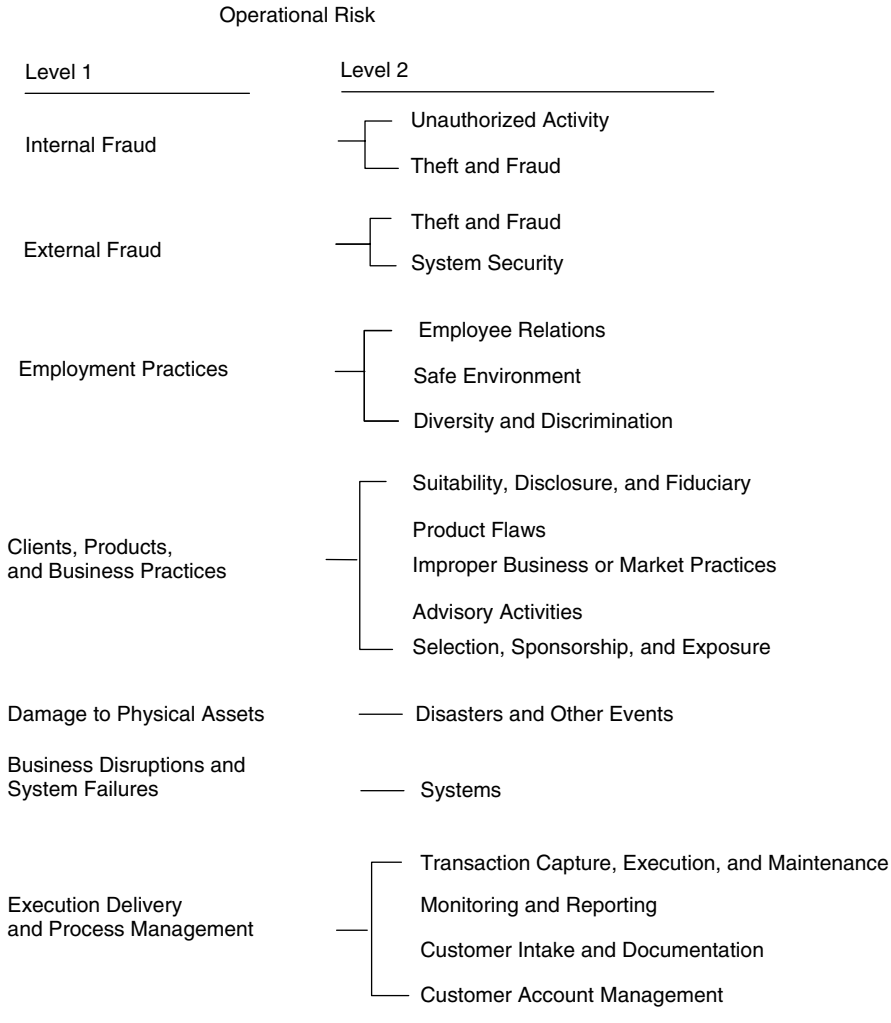


EXHIBIT 14.1 OPERATIONAL RISK CATEGORIZED

14.2 DEFINING OPERATIONAL RISK

The organization comes to a consensus as to boundaries and scope of operational risk and its management.

- The organization has defined operational risk management on an enterprise-wide level and is able to explain and defend its definition against peer organizations, regulations, and best practice frameworks.
- The organization has agreed on the boundaries to operational risk (e.g., whether it excludes or includes credit, market, legal, and reputational risk).
- The organization understands how operational risk may impact the quality and stability of earnings.

14.3 TONE AT THE TOP AND CORPORATE CULTURE

The organization's board and executive management have embraced operational risk management as a continuous process that is critical to meeting the organization's objectives.

- The board of directors has demonstrated its full support for operational risk management (ORM).
- The board and senior management have designed an overarching risk management policy that includes objectives and responsibilities.
- The board has created a risk management committee (RMC) that is chartered to perform active oversight of the firm's risk management framework. In financial institutions this should be separate from the audit committee due to the operational risk complexities and regulatory requirements coming with the Basel II capital accords.
- The board has ensured the alignment among the organization's business objectives, revenue drivers, and its risk exposure and appetite.
- The board reviews various risk alternative scenarios, such as worst and best case presented with alternative scenarios for the future financial results of the firm.
- There is a chief compliance and risk officer as a minimum and ideally both a risk officer and a compliance officer.
- There is a management consensus as to the main drivers around operational risk.
- There is a management consensus as to the benefits in improving operational risk management, such as reducing operating costs and losses, improving pricing accuracy, lowering financing and insurance costs, improving competitive position in the marketplace, and achieving greater stability in earnings.
- The organization has an ongoing process to assess and track the benefits of improved operational risk management.
- The organization understands the constraints to improving operational risk management such as budget constraints, inconsistent management support,

and issues in creating a cost versus benefit business case in favor of improving operational risk management.
- The organization understands its main ORM weaknesses and has compared them to their peer organizations and the best-in-class organizations.
- The organization has invested in high-caliber management with the skills, training, compensation rewards, and resources to improve ORM.
- The organization has embraced control and problem-fixing frameworks such as Enterprise Risk Management (COSO 2004) and six sigma.

14.4 DOCUMENTATION

The organization has a created, maintains, and reviews risk profile documentation approved by the board of directors that includes:

- Key performance indicators (KPIs)
- Key risk indicators (KRIs)
- Scorecards
- Benchmarks
- Business continuity planning
- Risk/control matrices (typically used in COSO-based regimes such as U.S. Sarbanes-Oxley, France's LSF, Germany's KonTrag, etc.)
- Stress testing and scenario analysis
- For financial institutions, a value at risk (VaR) analysis

14.5 POLICIES AND PROCEDURES

The organization has in place policies and procedures that encompass all business processes and technical functions that impact operational risk.

- The organization has in place a consistent and enterprise-wide process for the creation, collaboration, review, approval, and training/certification for these policies and procedures.
- These policies and procedures are published online and made available to employees, customers, suppliers, and regulators.

14.6 INDEPENDENT AUDIT

The organization has the trained staff, test protocols, and budget to support a robust internal and independent audit of all activities supporting operational risk management.

- The organization has regular independent reviews of all critical systems and procedures that impact operational risk.
- The independent reviews include a complete audit trail and a system of findings and recommended changes.

- The independent audit findings are reviewed on a regular basis by the risk and audit committees.

(a) BUSINESS RESILIENCY PLANNING (BRP). The organization has in place true business resiliency plans that address all potential business disruptions—much more than traditional disaster recovery programs that were limited to information technology disruptions.

- The organization has in place business resiliency plans (BRPs) that include disaster recovery from natural and man-made disasters.
- The BRP includes time lines, resources, tasks, and costs to get the organization up and running again.
- The BRP includes an analysis of critical outsourced processes.

14.7 MANAGEMENT OVERSIGHT

The organization has embraced all the needed oversight activities to mitigate risks in such a manner to meet the organization's objectives.

- The organization has a sound management control environment that includes segregation of duties, application and database controls over transactional and master-level data, and physical and logical controls over assets and data.
- The organization has identified potential high-risk areas and implemented the appropriate enhanced monitoring and management.
- The organization enforces an active rotation and forced vacation policy. (This has been shown to prevent fraud and expose internal control failures.)
- The organization enforces strict documents and records management that requires publication, access, and version control of all sensitive information.
- The organization has controls and incentives in place to support reporting and whistle-blowing with regard to fraud and unintentional errors.
- The organization has viable programs in place to detect and investigate untoward or suspicious behavior.
- The organization exercises the same level of control over outsourced activities that impact financial reporting as it does over internal activities.
- The organization fully supports and reinforces a moral and ethical culture that includes transparency and openness, and does not tolerate the hiding of mistakes or unethical behavior.
- The ethics policy clearly describes expected business conduct standards and actions to be taken when there are lapses. The policy makes it clear that every actor is responsible for preventing and detecting fraud, corruption, or unintentional errors. This policy is shared with customers, suppliers, and the community.

CHAPTER 15

THE USE OF SIX SIGMA IN OPERATIONAL RISK AND REGULATORY COMPLIANCE: REDUCTION IN VARIABILITY

Brett Trusko, PhD, Master Six Sigma Black Belt

Six sigma is often used as a catalyst for compliance and as a best practice in operational risk management, which is at the core of many compliance protocols. The criticality of compliance for numerous reasons, including physical and financial loss as well as the risk to the reputation and financial going concern of a company, means that companies are becoming more serious about the control that is obtained from adopting, or at a minimum utilizing, the tools of six sigma.

At the root of six sigma is the need to reduce variation in business processes. In fact, the term *sigma* refers to a standard deviation; for those who still remember their college statistics, the chance of a defect under a normal curve at six standard deviations is a number approaching zero. In the case of a company that must meet compliance requirements and is at risk for fines, or worse, less deviation means better consistency in reporting and thereby less risk for the company.

Many companies that are required to meet the regulatory compliance to reduce risks have also been interested in six sigma, and are finding that the two programs are complementary. Six sigma has been identified as a best practice in operational risk, which is core to almost all compliance initiatives. Done in concert, six sigma (generally considered a source of capital) will allow a company to improve internal processes and efficiencies while also improving legislated

compliance (generally considered a net use of capital). Since you have gotten this far into the book, we assume you have a strong understanding of regulatory compliance requirements to reduce risks, so this chapter focuses primarily on six sigma and leaves it up to readers to decide how best to apply it to their stage of compliance.

15.1 WHAT IS SIX SIGMA?

Six sigma refers to the Greek letter sigma (σ), which represents variation or variability. Consider your business; if you are producing a widget, you would like each widget to be produced in exactly the same way regardless of the time of the day, day of the week, and week of the month. If you deliver (or purchase) a service, it is important that the service be of consistently high quality, with the key being consistency. Now consider the need under many regulations to deliver on financial and reporting requirements. Given the high cost of regulatory failure, consistency (or lack of variation) is a highly desired state. This is a prime consideration in a joint compliance/six sigma approach.

The term *six sigma* indicates that a process is performing at a level where there are only 3.4 errors per million opportunities. In real-world terms, this means that 99 percent good (a traditional standard in business) is no longer good enough. The new standard is 99.99996 percent, as shown in Exhibit 15.1.

Of course, in terms of processes that feed regulatory compliance, there may never be a million opportunities for error. From a six sigma perspective, this

99% Good (3.8 Sigma)	99.99996% Good (Six Sigma)
20,000 lost articles of mail per hour	Seven articles of lost mail per hour
Unsafe drinking water for almost 15 minutes per day	One unsafe minute of drinking water every seven months
5,000 incorrect surgical operations per week	1.7 incorrect surgical operations per week
Two short or long landings at major airports every day	One short or long landing at major airports every five years
200,000 incorrect drug prescriptions each year	68 incorrect drug prescriptions each year
No electricity for almost seven hours each month	One hour without electricity every 34 years
11.8 million shares incorrectly traded on the NYSE every day	4,021 shares incorrectly traded on the NYSE every day
Three warranty claims for every new automobile	One warranty claim for every 980 new automobiles
48,000 to 96,000 deaths attributed to hospital errors each year	17 to 34 deaths attributed to hospital errors each year

EXHIBIT 15.1 HOW GOOD?

is good since as the number of opportunities decreases the chance of an error (noncompliance) decreases as well—to almost zero.

Six sigma consists of several components that are also complementary to the implementation of a regulatory compliance program in an organization. Six sigma:

- is a *management philosophy* and culture that passionately embraces defect-free process performance across the business;
- is a *disciplined, fact-based problem-solving methodology* that focuses on producing reliable and consistent results that meet customer and stockholder expectations; and
- is a *stretch goal*. Six sigma companies strive to deliver services, products, and profitable results, consistently within expectations—*every time*.

From the perspective of regulatory compliance, the development of a culture that is passionate about the elimination of defects is also less likely to tolerate errors that may make a company noncompliant. While processes can be implemented, a culture that is tolerant of errors is one that ignores errors and/or doesn't expose them when they do occur.

The fact-based, problem-solving methodology is needed to identify where processes are breaking down, what they cost, and which processes are the priorities for the organization. The methodology uses data and facts to address process inadequacies instead of feelings or intuition about where a problem lies. In a compliance program, merely guessing at where processes are or might break down is too high a risk to be managed on intuition.

No process can function without occasional failure. As a leader with responsibility for regulatory compliance, this should concern every compliance officer, executive, and board member. As a mitigation strategy, adoption of a six sigma program and its emphasis on stretch goals communicates to stakeholders that your organization is interested not only in meeting minimum requirements, but in going beyond to as close to perfection as possible.

15.2 THE SIX SIGMA METHODOLOGY

Six sigma sounds a bit like a karate exercise. There are various titles indicative of the level of training and experience that a practitioner has achieved or obtained. The most typical titles heard in six sigma are process owners, champions, green belts, black belts, and master black belts. How organizations use these individuals can vary from organization to organization, but generally their responsibilities are:

- *Process owner*. This individual is responsible for a process. This is a foreign concept to many organizations, but in a six sigma organization all identified processes should have a process owner. Their job is to define the process and monitor the continued success of the process they own.

- *Champion*. This individual could be the process owner. Generally champions are executives in the organization who support the program and members of the team. They would be expected to negotiate with other managers when a problem spans multiple silos or departments.
- *Six sigma green belt*. This person is a part-time employee who has undergone one to two weeks of training in the six sigma methodology. These individuals will typically spend approximately 25 percent of their time working on six sigma projects.
- *Six sigma black belt*. This person is a full-time employee who is essentially the project manager in a six sigma project. They typically have undergone extensive training, generally up to eight weeks of classroom and field training covering problem solving and statistical methods.
- *Master six sigma black belt*. This individual is a full-time employee who has the responsibility to manage the education, training, and promotion of the program. In my experience, this individual might be either a statistics expert or a change management executive, depending on the orientation and needs of the organization.

The six sigma methodology consists of five steps that depend on whether the organization is attempting to improve an existing process or is creating a new process. The improvement process's five-step methodology is:

1. Define
2. Measure
3. Analyze
4. Improve
5. Control

The new process methodology (DMAIC) replaces Improve and Control with Define, Measure, Analyze, Design, and Validate (DMADV). For this discussion we will not cover DMADV.

A key point to remember when doing a six sigma project is that the DMAIC project should last only 12 to 16 weeks (which requires a small, well-defined project), whereas a DMADV or redesign might take years.

A key component of the six sigma program and the DMAIC process that will also be discussed are tollgate reviews. Exhibit 15.2 shows a typical six sigma program.

Tollgate reviews are typically stopping points to evaluate whether the project is progressing as planned. For example, at the end of the define phase, one would stop and review with the compliance committee whether the problem is well understood, the team is properly identified, and all components of the project are mapped out and communicated. At the end of the measure phase, the group would evaluate whether the right measurements were performed, enough information was gathered, and so on.

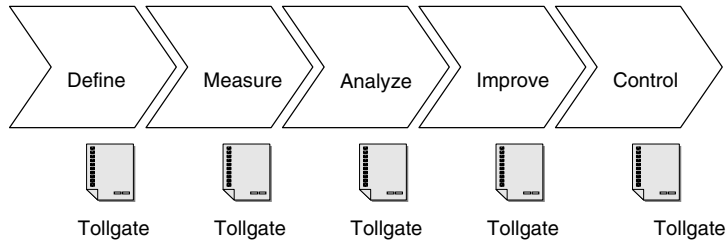


EXHIBIT 15.2 THE DMAIC METHODOLOGY

(a) DEFINE. The define phase of the methodology focuses on understanding the process, what it does, why it does it, and what the customer wants. The understanding is typically referred to as "critical to quality," but since the customer can have many faces—the end customer, the internal customer, or, in the case of the Sarbanes-Oxley Act (SOX) compliant corporation, the shareholders and governmental regulators—and because this book is about compliance, for the remainder of this chapter we refer to the compliance stakeholders as the voice of compliance (VOC).

In the context of the define stage, VOC requires the organization to fully understand the requirements of the SOX stakeholders as well as the processes that create the product that are critical to the customers of the compliance effort. The define stage allows the organization to embark on SOX with a clear definition of what is critical to the customer (VOC), as well as assumptions of how and where the organization is currently failing. The whys of failure are taken up in later stages of the DMAIC process; in this stage we are most interested in defining our problems and the processes that contribute to a successful compliance program.

(b) MEASURE. The measure phase in six sigma requires the six sigma team to identify the processes enabling the VOC and gather data specific to those processes. In this phase the VOC is identified as "Y." Given that the Y is the output of the process, whether that is an internal process, an external process, or a statutory reporting requirement, six sigma reminds us that for every output Y there is a series of "x's." In a process, an x is anything that affects the output. This means supplies, people, computer systems, transformative processes, and anything else that contributes to the creation of the end product, Y. Accordingly, six sigma uses the formula $Y = f(x)$, which simply means that Y is a function of all the x's that go into the creation of Y. And, as everyone knows, while there may be hundreds of x's in a transformative process, there are only a vital few that actually have a significant effect on the output.

The measure phase attempts to identify what is important to the output and what transformation takes place, and measures those transformative x's that are

subject to variation. Upon measuring the vital few x's, the organization has a basis to move to the next phase and analyze both the variation in the x's and the effect that those variations have on the output Y.

(c) ANALYZE. The analyze phase of the six sigma methodology is the one that intimidates many and chases others away from the program. Whereas advanced statistics can be used in the analyze phase, many, if not most, times a few simple tools and concepts can accomplish as much as sophisticated statistics.

The first of these tools is the normal curve, or normal distribution. In short, referring to Exhibit 15.3, the normal curve represents the probability that some event will take place. Six sigma gets its name from the fact that at six standard deviations, the probability that an event will happen, say a form with an error (or defect) on it, is so low as to be almost impossible. In the six sigma world, out of a million forms, one would expect only 3.4 errors.

Since we already know that we cannot actually change the Y's in the $Y = f(x)$ formula, the specification limits will fall somewhere in the normal curve. How tightly the curve is bunched determines if there is a 64 percent chance of a form with errors or something as insignificant as 3.4 per million in a six sigma capable process.

Other tools used in six sigma are referred to as the basic tools and are:

- Descriptive statistics
- Histograms
- Pareto charts
- Line and run charts

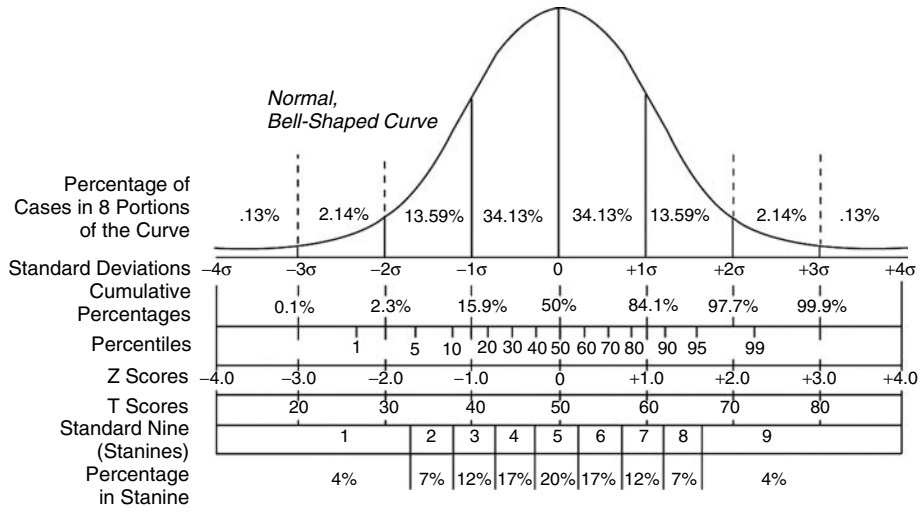


EXHIBIT 15.3 THE NORMAL CURVE

- Scatter plots
- Control charts

While these tools are not all used in this phase, they can be done easily with a simple statistical analysis program such as Microsoft Excel or many other off-the-shelf software packages. For a better description of the tools, it is advisable to hire any of the outstanding six sigma consultants available today to train your executive team as six sigma champions, a simple one-day course on the basics of six sigma.

Regardless, the analyze phase allows us to very specifically identify where variation is happening and how it is affecting the output of our process in dollars and, for the compliance professional, risk.

(d) IMPROVE. The improve phase is just as the name implies: time to apply the findings of the analyze phase to the vital few x's that cause variation in the process. In this phase we pilot and implement the mitigation or process modification that is necessary to eliminate variation. In the pilot, we test the improvements, take additional measurements, do additional analysis, and eventually arrive at the point where we are convinced that our pilot will improve the process to the point that the naturally occurring variation is significantly reduced, at least so that the additional cost of improvement is balanced with the risk.

Which brings us to another statistics fact: Six sigma recognizes that there are two types of variation—variation caused by nature (common cause variation) and special cause variation. Common cause variation is the variation that is caused by machines wearing down, mild human error intrinsic in the human condition, and other variation generally out of our control. Special cause variation is variation that is caused by more unusual occurrences such as tampering, a broken machine that goes down, and other events that can generally be planned for and must be eliminated if a process is to remain in control. Six sigma always addresses special cause variation before tackling common cause variation.

At the conclusion of the improve phase, the process modification has been piloted, measured, and analyzed with the practitioner concluding that variation has been reduced to a level that is acceptable to the organization. It is then that a full-scale implementation is done on the revised process. Remember that in this phase we will not achieve performance in the entire process of 3.4 errors per million; however, we can design the process to achieve something like that in key x's in the process, such as a signature, a footed column of numbers, or a critical filing date. There might still be a misspelled word, but that isn't typically a "vital few" item required by the customer.

(e) CONTROL. Too often in management a process is improved or put in place only to be forgotten. In the control phase of six sigma we implement a system that is intended to assure us that an improved process remains in control. We utilize run charts, line charts, and statistical process control (SPC). We identify

a process owner who continuously monitors the process to be sure that the six sigma team is called back in when processes are out of control.

Finally, expect your six sigma team to celebrate success. Six sigma is meant to be a culture-changing experience that is intended to foster an environment of continuous improvement and an eye for quality. If done well, employees are allowed to challenge the status quo and bring up problems they identify before they become significant.

15.3 THE HARD TOOLS OF SIX SIGMA

As one can surmise from the discussion thus far, six sigma, in a quest to reduce variation, utilizes basic statistical theory and solutions to improve process performance. As mentioned earlier, there are a few basic concepts that even the worst statistiphobe should be able to navigate in understanding the basics of six sigma.

The first of these tools is descriptive statistics. As you will recall from earlier in the chapter, the normal distribution (or curve) is a basic premise in six sigma. As a simple example, if you were to take two dice and roll them, you would have a 6 in 36 (16.66 percent) chance of rolling a 7 and only a 1 in 36 (2.7 percent) chance of rolling snake eyes. If you were to throw dice for an extended period of time and plot the results, you would find a normal curve that would accurately reflect the fact that your best chance of winning a bet is on 7. (See Exhibit 15.4.)

Descriptive statistics tell us about the shape of a curve and accordingly allow us to understand the probability that a process would be noncompliant. In the case of the dice example, suppose that a 2 or a 12 is a defective roll or an incident of noncompliance in a process. The descriptive statistics are shown in Exhibit 15.5.

The descriptive statistics for this very limited set of numbers tell us exactly what we already know about the small set. The interpretation of a limited number of rolls of the dice is not important to know, but what is important is that in a sample of compliance-related transactions, we can expect certain behaviors. When

	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

EXHIBIT 15.4 PROBABILITY IN THE ROLL OF DICE

Mean	7
Standard Deviation	2.44949
Variance	6
N	36
Minimum	2
1st Quartile	5
Median	7
3rd Quartile	9
Maximum	12

EXHIBIT 15.5 DESCRIPTIVE STATISTICS

we understand the descriptive statistics about a process, we can more easily see when an unusual item is caused by random variation or a special cause, such as tampering.

The second hard tool of six sigma is the histogram. Exhibit 15.6 shows a histogram of call pickup times in a call center. The histogram is useful because it shows the distribution of a sample. As you might notice, the call pickup time curve is normally distributed (you could draw a normal curve on top of the pickup times). If we were to find a point far to the right or left, a downward trough in the middle, or some other anomaly, we would want to investigate why this is occurring. In the process of investigation we would better understand our process and be able to refine the process as indicated.

The third hard tool is the Pareto chart. Most people know the Pareto principle as the 80/20 rule, which is that 80 percent of your errors occur in 20 percent of your transactions. While this is not a definition of the Pareto chart, it does tend to show on the left of the chart with a cumulative line working its way up

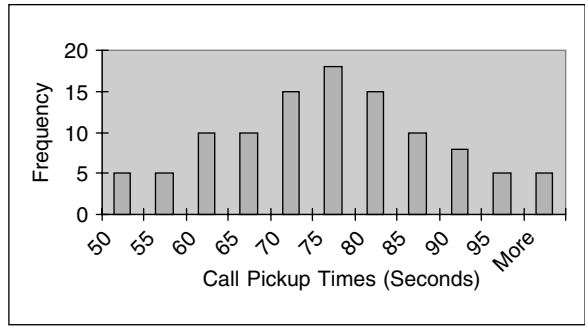


EXHIBIT 15.6 HISTOGRAM OF CALL PICKUP TIMES

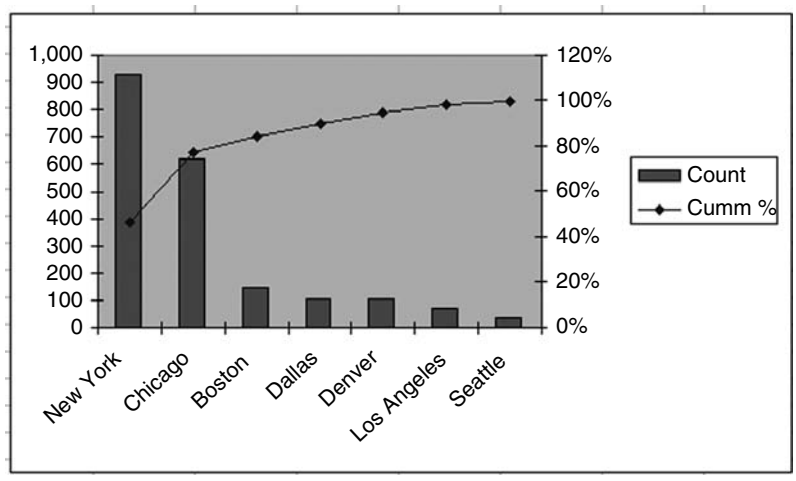


EXHIBIT 15.7 PARETO CHART

and to the right. The Pareto chart is used to identify where the greatest number of errors occur or what they are.

In the case of Exhibit 15.7, we see that New York has the highest number of something. If this happens to be a certain type of error, then we need to investigate why this is happening. If New York happens also to be the busiest location, we can weight the Pareto chart to account for relative size.

Line and run charts are simple tools for tracking something over time. Exhibit 15.8 shows a simple line chart of cycle time for some process. A line chart is particularly useful in spotting trends in a process. In the example, we might want to investigate why there are numerous spikes near the middle. In a compliance example, we may want to know when an untrained individual is part of a process, so would like to investigate spikes such as those shown. An expert might point out subtle differences between line and run charts, but for the purposes of this discussion they are not important.

Scatter plots demonstrate the correlation of two variables to each other. As most people who have had algebra in college can recall, a scatter plot can show a positive or negative correlation and everything between. Exhibit 15.9 shows a scatter plot with a strong positive correlation between two variables. In the case of a compliance program, we might like to understand if there is a correlation between the day of the week and errors, or perhaps employees and errors. The variables that can be explored and monitored are vast and limited only by one's imagination.

The control chart may be the most useful tool in the compliance manager's tool kit. A control chart (Exhibit 15.10) is a run chart with a few key differences. First, the control chart identifies the mean of some process. Then, utilizing

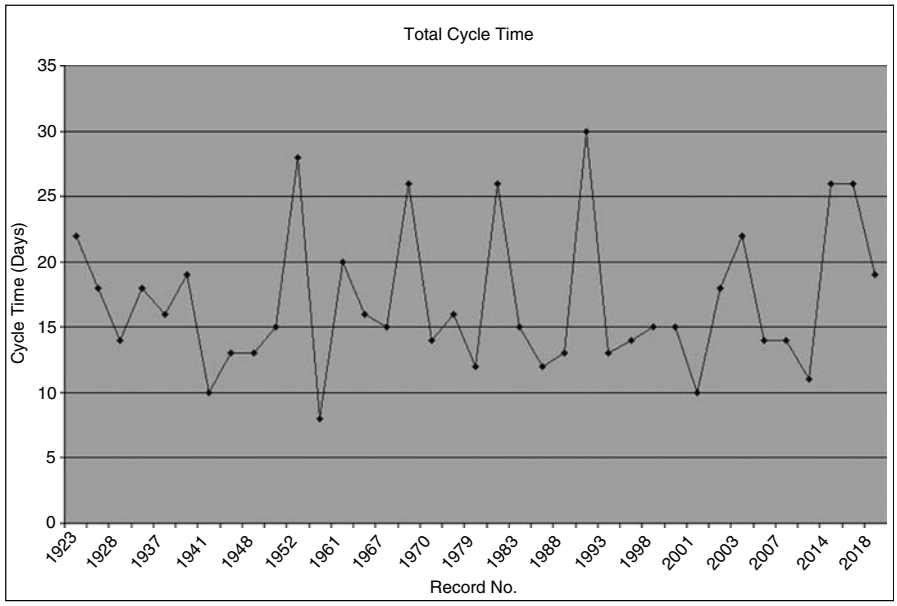


EXHIBIT 15.8 LINE AND RUN CHART

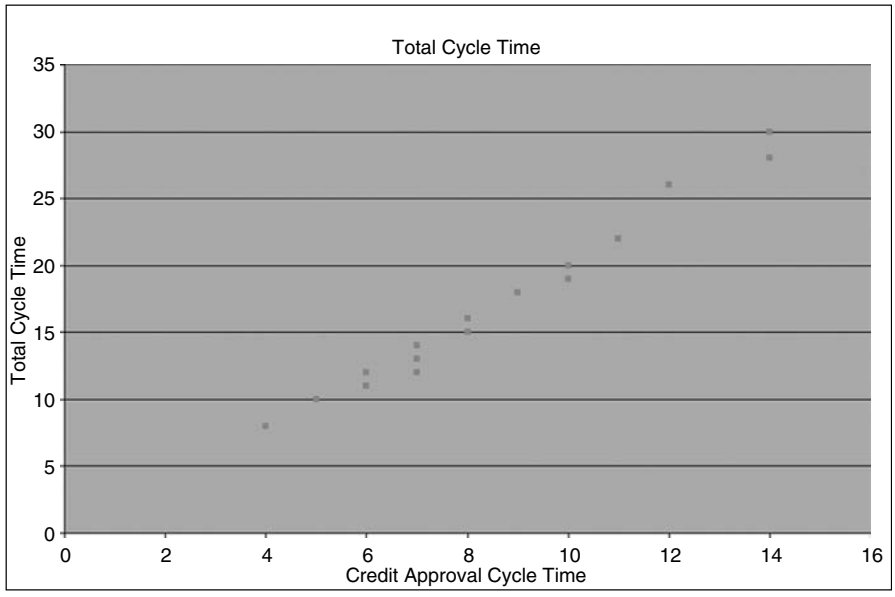


EXHIBIT 15.9 SCATTER PLOT

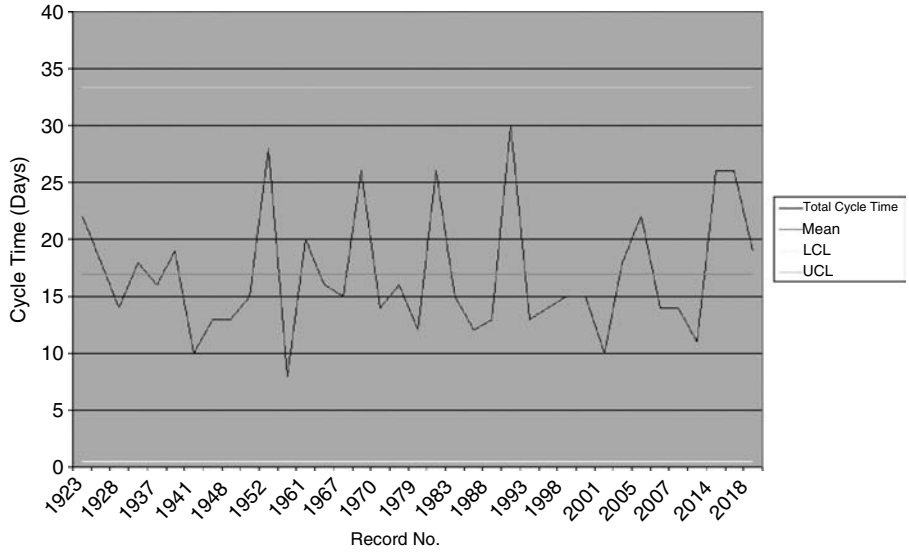


EXHIBIT 15.10 CONTROL CHART WITH UPPER AND LOWER CONTROL LIMITS

descriptive statistics, it calculates the standard deviation. Now, since we understand that 99.9 percent of all sample measurements should occur within three standard deviations, we can surmise certain things about the control chart and those are:

- Any point falling outside of three standard deviations must be an abnormal occurrence (or a special cause) that should be investigated.
- Any trends that would not be expected to occur in nature (randomly) should be investigated. These trends include:
  - One or more points outside the control limits (three standard deviations)
  - Two out of three consecutive points on same side of the centerline between the 2 S.D. line and the control limit
  - Four out of five consecutive points on same side of the centerline between the 1 S.D. line and the control limit
  - Fifteen consecutive points hugging the average
  - Eight points in a row between the 2 S.D. line and the control limit on either side of the centerline

Each of these trends would be unnatural and in our experience occur when machines are not functioning properly, individuals are tampering with processes, suppliers are not meeting specifications, or any number of other unnatural causes.

Now, add to the control chart the requirements demanded of the process. In six sigma we refer to these as specification limits. In the compliance world, these are the requirements of the compliance body. Specification limits are superimposed on the control chart (and the normal curve) to show how well the process is performing against the customer requirements (the customer being the regulatory body).

If we are performing within three standard deviations of the mean but not performing within the specification limit, we are said to be incapable but in control (not able to consistently produce to our customer requirements), in which case we must modify our process to meet those customer expectations. If, in a compliance program, we cannot meet the customer expectations, it is possible we are breaking some law.

If the line for the specification is outside the control limit line, we are then generally only subject to processes that are not in control but are capable—a much better situation than in the "in control" but "not capable" example, because we are at least meeting the customer expectations and assumed to not be breaking any compliance rules. One would be cautioned, however, that if a process is capable but out of control there is a high risk that the process could easily find itself out of compliance.

Therefore, the process related to some compliance procedure is at its best when it is both in control and capable, because we are producing what the customer is asking for in a consistent manner. Note that this does not necessarily mean that the process is operating at a six sigma level. In fact, it is possible that producing at 99.9 percent accuracy is the best we want to do as higher levels of compliance are too expensive given the little added protection they afford.

15.4 THE SOFT TOOLS OF SIX SIGMA

Many people reject six sigma as a giant statistical solution to the company's problems with variation. While this is partially true, it is important not to be scared off by the math. A significant benefit that six sigma offers the organization is the soft skills that many six sigma professionals deemphasize in certifying professionals. Some of these soft tools include a disciplined approach to improving processes. While you will want to seek guidance from your legal council, one cannot help but feel that a well-organized quality program such as six sigma, with its documentation requirements and training, is more easily defensible should you be called to court.

An additional soft tool is the process of understanding the voice of the customer (VOC). From the compliance perspective, and while training employees may be mandatory in a compliance program, the VOC allows individuals working on a compliance process to really understand why the compliance requirements exist, and in doing so better understand compliance than one who simply takes a 30-minute online class.

Traditional Model	Six Sigma Goals
• Intuition-based decision making • Reliance on trial and error • Dependence on rework • Fixing • Accepting firefighting behavior • Point or one-off solutions • Minimal tracking of post-implementation results	• Metric-driven organization • Structured methodology • Defect-free processes • Preventing • Challenging status quo • Integrated solutions based on customer and business needs • Ongoing monitoring with corrective actions

EXHIBIT 15.11 ORGANIZATIONAL APPROACHES

Other benefits include team-building knowledge that is a critical part of the certification process, as well as evolution to a quality-driven organization that emphasizes and values metrics over intuition, structure over trial and error, prevention of errors over inspection, and rework and permanent preemptive solutions over firefighting and one-off fix behavior. (See Exhibit 15.11.)

15.5 CONCLUSION

If you haven't connected the dots on why six sigma is important to the corporation that is subject to demanding regulatory compliance, it can be summed up in one word—variation. As an executive, variation in your corporate books can be a frightening proposition. No one wants to make errors, and a few minor errors are understandable. Major errors, however, are unacceptable to shareholders, governing bodies, and employees.

A six sigma program can help in several ways. First, reduction in variation means that what the compliance program is supposed to produce on a consistent basis is produced more consistently; in a compliance program, getting what you expect is the key. Second, if errors happen, and they might, it is much more defensible to parade out a six sigma initiative with proven due diligence that might have failed than to throw up your hands and say, "We did our best."

Six sigma will allow a more consistent compliance program consistently. Consistency and meeting expectations may seem boring, but in the compliance world boring, consistent, and predictable are good things.

CHAPTER 16

OPERATIONAL RISK MANAGEMENT USING QUANTITATIVE METHODS

Deborah Cernauskas, PhD
Koti Ancha, Six Sigma Black Belt

16.1 INTRODUCTION

The Merriam-Webster English Dictionary defines *risk* as "The possibility of loss or injury" or "Someone or something that creates or suggests a hazard." Risk management is the process of identifying, measuring, or assessing risk and then developing strategies to manage/mitigate the risk.

Even though the word *risk* has a negative connotation, the outcome of taking risks can be either positive or negative. Individuals and corporations take calculated risks to achieve their goals and objectives. There are several types of risks that are identified with different industries or organizations (i.e., market,

credit, insurance, legal, strategic, regulatory, technology, health, etc.). Risk is any internal or external event that may impede enterprises, for profit or not for profit, from achieving their goals and objectives. In any typical enterprise, external risks are far better managed than internal risks. This is due to the fact that a lot of emphasis is put on monitoring, evaluating, and managing external sources of risks. Almost all of the well-publicized corporate scandals can be attributed to failures in identifying and managing internal sources of risks. The Basel Committee on Banking Supervision (BCBS[1]) published papers titled "A Framework for Internal Control Systems in Banking Organizations" (1998) and "Sound Practices for the Management and Supervision of Operational Risk" (2003), which laid the foundation for managing operational risk for financial institutions. Basel II defines operational risk as the risk of losses resulting from inadequate or failed internal processes, people, and systems or from external events. This definition holds true for any industry. Over the past couple of years, compliance-related regulations and the need for better transparency in corporate reporting have highlighted the need for implementing processes and tools that help with governance, risk, and compliance (GRC).

Operational risk is an issue for all companies, but its scope is so vast that it is hard to define and equally hard to measure. Operational risk is generally characterized as those risks related to business, crime, disaster, information technology, and regulatory compliance, but it excludes strategic processes. It is the hardest risk to anticipate and has the potential to be of devastating magnitude to the finances of the company. Although operational risk has always been an issue for firms, the quantification of operation risk has come to the forefront since Basel II's inclusion of a capital charge for operational risk.

Whereas Basel II treats market, credit, and operational risk as independent events, in a trading firm operational risk, which generally arises from human and technological errors, can easily transform itself into market and credit risk. Consider that in 1995, Barings PLC declared bankruptcy due to the actions of a single trader who lost $1.3 billion in derivatives trading. The derivatives market risk Barings succumbed to was due to a lack of proper controls, an operational risk. Of a lesser magnitude, in 2006 a well-known Chicago investment company placed numerous trades in error when a row was added to an Excel spreadsheet, causing the logic of the model to fall apart. The latter example is very common in trading environments.

Currently, many industry professionals and academics are struggling to identify and quantify the numerous risks that fall under the canopy of operational risk while there is a scarcity of data available. Modeling efforts to quantify operational risk will not be very successful until adequate data are available. To this end, over the past couple of years, some companies and consortiums have been actively compiling loss databases. The Association of British Insurers (ABI) set up one such consortium, the Operational Risk Insurance Consortium (ORIC), in November 2005. Companies such as Wachovia are finding the internal data

hard to collect, since the data are kept in organizational silos.[2] Each internal Wachovia organization has a system and process to capture, collect, and store the data. The integration and validation of the data have presented many challenges in Wachovia's development of a risk framework.

A lot of material has been written on the subject of Enterprise Risk Management (ERM), which is a framework that helps companies in their efforts to better gauge and manage risks. The Committee of Sponsoring Organizations (COSO)[3] ERM framework defines essential ERM components, discusses key principles, and proposes a common, effective ERM language. The framework defines ERM in part as follows:

> Enterprise Risk Management is a process effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Most large companies have risk management processes in place, and they know that taking risks is part of doing business and that managing risks is critical to their success. In spite of this, there is still a huge gap in the area of operational risk management. The onus is placed on the individual functional areas to manage these risks, as opposed to an enterprise approach.

16.2 DEFINING OPERATIONAL RISK

Basel II defines operational risk as the risk of losses resulting from inadequate or failed internal processes, people, and systems or from external events. The definition includes legal risk but excludes strategic risk and reputation risk. Even though the Basel committee addresses the banking industry, the underlying fundamentals can be applied to any industry or organization. Basel II believes that deregulation, globalization, and growing sophistication of financial technology are making the activities of banks and thus their risk profiles more complex. The same can be said of any type of business (i.e., manufacturing, mining, health care, food and drug, etc.). Some of the examples mentioned in the paper are:

- Greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks.
- Growth of e-commerce brings with it potential risks that are not fully understood.
- Large-scale acquisitions, mergers, demergers, and consolidations test the viability of new or newly integrated systems.
- The emergence of banks acting as large-volume service providers creates the need for continual maintenance of high-grade internal controls and backup systems.

- Banks may engage in risk mitigation techniques (e.g., collateral, credit derivatives, netting arrangements, and asset securitizations) to optimize their exposure to market risk and credit risk, but which in turn may produce other forms of risk (e.g., legal risk).
- Growing use of outsourcing arrangements and the participation in clearing and settlement systems can mitigate some risks but can also present significant other risks to banks.

The term *operational risk* carries different meanings to different organizations. No matter how a particular organization defines operational risk, a clear understanding of what is meant by operational risk is critical to the effective management and control of this risk. Any of the following events categorized as operational risks can result in substantial losses:

- Internal fraud (e.g., employee theft, insider trading, etc.)
- External fraud (e.g., robbery, forgery, check kiting, and computer hacking)
- Employment practices and workplace safety (e.g., workers' compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability)
- Clients, products, and business practices (e.g., fiduciary breaches, misuse of confidential customer information, improper activities on the bank's account, money laundering, and the sale of unauthorized products)
- Damage to physical assets (e.g., terrorism, vandalism, earthquakes, fires, and floods)
- Business disruption and system failures (e.g., hardware and software failures, telecommunication problems, and utility outages)
- Execution, delivery, and process management (e.g., data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, nonclient counterparty misperformance, and vendor disputes)

The Basel II framework outlines the development of an appropriate risk management environment; risk management (identification, assessment, monitoring, and control/mitigation); the role of supervisors; and the role of disclosure.

16.3 DEFINING QUANTITATIVE ANALYSIS (QUANTITATIVE METHODS)

Quantitative analysis refers to the use of numerical and statistical techniques rather than the analysis of verbal material. Quantitative analysis is data driven, and data is central to everything. As the saying goes: If you can't express something in the form of numbers, you really don't know much about it; if you don't know much about it, you can't control it; if you can't control it, you are at the mercy of chance, and hence why bother with it?

Market, credit, and insurance risks rely heavily on statistical analysis of historical data for quantification. There is enormous amount of historical data

available in this space, and a number of sophisticated tools are available for modeling complex scenarios to understand and mitigate risk. The same cannot be said for measuring, modeling, and managing operational risk. It is not always easy to collect data on each and every process, and even if there is data being collected it may not be in the desired format or may not meet the needs of quantitative analysis.

16.4 ADVANTAGES AND DISADVANTAGES OF USING QUANTITATIVE METHODS

Quantitative analysis produces statistically reliable and generalizable results. Data are classified and counted, and statistical models are constructed to explain what is being observed. Findings can be generalized to a larger population, and direct comparisons can be made between two different sets of data or observations. Quantitative analysis allows us to discover which phenomena are likely to be genuine and which are merely chance occurrences. If the underlying cause of a particular behavior or trend is understood, then appropriate measures can be put in place to change the behavior to reflect the desired state.

However, it is not always easy or possible to collect data on a certain process; and even if it is possible to collect data, the numbers might not tell the whole story. For statistical purposes, classifications have to be "yes" or "no," "in" or "out"; and this kind of analysis can produce results that may not provide the real perspective on a problem.

16.5 OPERATIONAL RISK ASSESSMENT AND MANAGEMENT—ESSENTIAL COMPONENTS

Operational risk management is a subject of great interest as risk managers are looking for ways to easily measure and manage operational risk. A lot of material has been published on this subject that helps define, identify, measure, and manage operational risk from an enterprise perspective. The spectrum of solutions covers a broad range, starting with the simple idea of identifying processes with risk and putting controls in place to mitigate the risk. On the other extreme there are quantitative risk management tools that can help with modeling techniques for quantitative risk management and help solve business problems.

It is not always the case that reliable historical data are available for analysis for any given process within an organization to quantify process failures and the risk induced by these failures. Six sigma methodology, which has gained a strong foothold in the business community as the most desirable process improvement methodology, relies heavily on data-driven analysis. One of the tools used within six sigma to design and implement a robust process is to identify failure modes and establish a risk priority so that corrective actions can be put in place to address and or reduce the risk. This tool is called failure modes and effects analysis (FMEA). FMEAs help in identifying and documenting where in the process the source of the failure impacts the customer (internal or external customer).

The following steps can be used as a guideline to assess and manage operational risk:

1. Identify key processes.
2. Identify and assess risk; conduct FMEA, business process modeling (BPM), simulation, and so on.
3. Quantify operational risk.
4. Monitor and control risk.

(a) IDENTIFY KEY PROCESSES. A typical business entity is comprised of several business processes that help run the business and achieve its goals and objectives. Not all of these processes are directly related to selling a product or revenue generating but indirectly contribute to the success of the organization and hence can definitely have an opposite effect as well. Not every process has the same impact, positive or negative, on the business, and hence it is important to identify key processes that need to monitored and managed from an operational risk management perspective.

(b) IDENTIFY AND ASSESS RISK. After identifying all the key processes, the next step would be identify and assess the risk posed by the process to the organization as a whole. Several methods can be used to identify and assess risk, but here are some methods that you can consider as appropriate for your business:

- Failure modes and effects analysis (FMEA)
- Business process modeling (BPM) and simulation

(c) FAILURE MODES AND EFFECTS ANALYSIS. FMEA is used to determine failure modes and assess risk posed by the process and thus to the organization as a whole. The outcome of this analysis will be a risk priority number (RPN). Generally, the higher the RPN, the greater the priority associated with fixing the cause of failure and thus reducing the overall risk to the organization. (See Exhibit 16.1.)

Exhibit 16.2 is an example of an FMEA form. Please note that different forms can be used, but most contain the same basic information.

The following steps are used to fill in the FMEA form so the team can begin the process of calculating a RPN. It is assumed that all the key processes are identified and a process flow for each of the processes is available to start this process.

1. Fill in the column labeled "Potential Failure Effects" with what might happen if there is a failure in this process step. There could be more than one potential failure effect in any given process step.
2. Identify potential causes for this failure and enter them in the "Potential (Root) Causes" column. These are the potential root causes responsible for the failure.

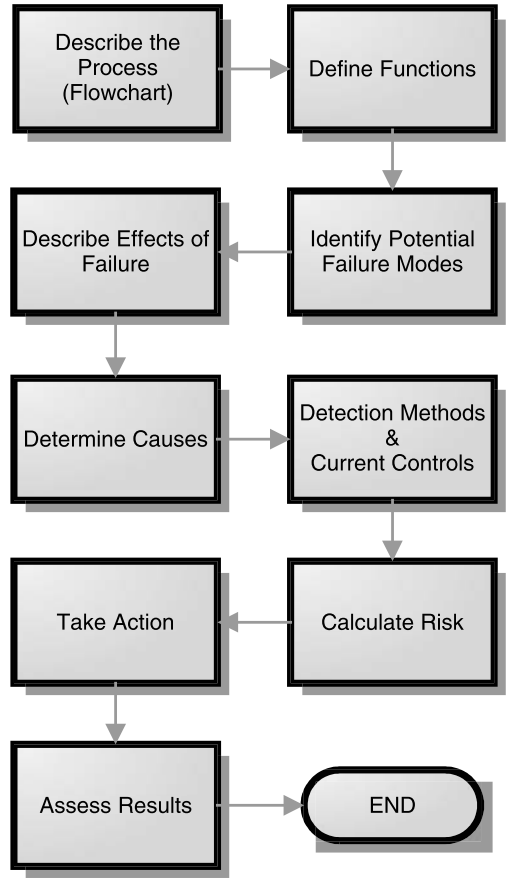


EXHIBIT 16.1 FMEA ROAD MAP

No.	Process Step	Potential Failure Modes	Potential Failure Effects	SEV	Potential (Root) Causes	OCC	Current Controls	DET	RPN	Recommended Corrective Action(s)	Action(s) Taken

EXHIBIT 16.2 EXAMPLE OF AN FMEA FORM

No.	Process Step	Potential Failure Modes	Potential Failure Effects	SEV	Potential (Root) Causes	OCC	Current Controls	DET	RPN	Recommended Corrective Action(s)	Action(s) Taken
1	Step 1	FM-1	Effect-1		C-1						
2	Step 1	FM-2	Effect-2		C-2						
3	Step 3	FM-3	Effect-2		C-3						
4	Step 5	FM-4	Effect-3		C-4						
5	Step 6	FM-5	Effect-4		C-5						

EXHIBIT 16.3 FAILURE MODE EVALUATION ANALYSIS (FMEA)

3. The task now is to link each identified potential cause with its corresponding process step. A potential cause could occur in more than one process step. And to complicate it further, multiple potential causes can occur in the same process step.
4. Identify the potential failure mode for each cause. For each potential cause, enter the corresponding failure mode on the FMEA form. A failure mode is a brief description of how a process could fail. It is usually the first thing that you will detect when something goes wrong in the process. Failure modes answer the question, "Can we catch the problem after the cause but before the effect?"

Exhibit 16.3 shows the completed failure mode evaluation analysis (FMEA worksheet).

Now it is time for the team to assess severity (SEV), occurrence (OCC), and detection (DET). If you've produced a detailed process map and have walked through the process, these assessments will be relatively easy. For each item, we use a scale of 1 to 10 from low rating to high rating. In normal circumstances, you will have your subject matter experts assist you with these ratings.

The SEV rating indicates how significant the impact of the effect is to the customer. Your team will use a severity rating chart to help you. A rating of 8 on the chart means the customer would have a very high degree of dissatisfaction if there is a loss of service. Exhibit 16.4 is an example of the scale used to assign SEV ratings.

The OCC rating determines how likely the cause of the failure mode is to occur. For example, from the occurrence rating chart, a rating of 9 indicates that a failure is almost certain, based on the data in Exhibit 16.5.

Before completing the detection rating (DET), the team might want to enter detailed information in the "Current Controls" column of the FMEA worksheet. Here you describe the methods you currently use to prevent or detect the failure modes or causes. Controls that prevent failure modes or causes from occurring are mistake proofing, automated control, and setup verification. The DET rating measures the likelihood that the current control system will detect the cause or failure mode if it occurs. On the rating chart in Exhibit 16.6, we see that a rating

Rating	Degree of Severity
1	Customer does not notice the adverse effect or it is insignificant
2	Customer probably experiences slight annoyance
3	Customer experiences annoyance as a result of poor service
4	Customer is dissatisfied as a result of poor service
5	Customer is made uncomfortable or its productivity is reduced by the continued poor service
6	Customer complaints as a result of service issue
7	High degree of customer dissatisfaction due to loss of being able to use a portion of the service
8	Very high degree of dissatisfaction due to loss of service
9	Customer has lost total use of service
10	Customer has lost total use of service and will never return

EXHIBIT 16.4 EXAMPLE OF SCALE USED TO ASSIGN SEV RATINGS

of 10 says there is absolute certainty that the current controls will not detect the potential failure.

With the severity (SEV), occurrence (OCC), and detection (DET) values determined, you can compute the risk priority number (RPN). (See Exhibit 16.7.) This is a numerical calculation of the relative risk of a particular failure mode. In other words, RPN equals SEV times OCC times DET. The purpose of the RPN number is to prioritize your potential causes. Higher RPN numbers require immediate focus and a solid control plan. Ideally, you would want to use mistake proofing, if at all possible. Elimination of the potential failure mode is always better than trying to detect the mode with controls.

The risk priority number (RPN) is a relative ranking of the risks associated with each potential failure. In this example, FM-2 poses the most risk for the team. It has a severity rating of 5 and an occurrence rating of 2, and there is

Rating	Likelihood of Occurrence
1	Likelihood of occurrence is remote
2	Low failure rate with supporting documentation
3	Low failure rate without supporting documentation
4	Occasional failures
5	Relatively moderate failure rate with supporting documentation
6	Moderate failure rate without supporting documentation
7	Relatively high failure rate with supporting documentation
8	High failure rate without supporting documentation
9	Failure is almost certain based on data
10	Assured of failure based on data

EXHIBIT 16.5 LIKELIHOOD OF OCCURRENCE

Rating	Ability to Detect
1	Sure that the potential failure will be found or prevented before reaching the next customer
2	Almost certain that the potential failure will be found or prevented before reaching the next customer
3	Low likelihood that the potential failure will reach the next customer
4	Controls may detect or prevent the potential failure from reaching the next customer
5	Moderate likelihood that the potential failure will reach the next customer
6	Controls are unlikely to detect or prevent the potential failure from reaching the next customer
7	Poor likelihood that the potential failure will be detected or prevented before reaching the next customer
8	Very poor likelihood that the potential failure will be detected or prevented before reaching the next customer
9	Current controls probably will not even detect the potential failure
10	Absolutely certain that the current controls will not detect the potential failure

EXHIBIT 16.6 DETECTION RATING CHART

only a moderate likelihood of identifying the failure (7) before it might escape. The team should review the current controls to enhance or search for methods to eliminate the cause of the failure by mistake proofing the process.

The team should document the corrective actions that could be implemented to address the root causes of the failure modes and select the corrective actions that should be implemented. As each corrective action is implemented, appropriate documentation should be maintained as to how this corrective action was implemented and the test results that show the effectiveness of the control.

(d) BUSINESS PROCESS MODELING AND SIMULATION. Although it may appear that most operational risks are preventable with the implementation of procedures and controls, it is not an easy task to identify and control all risks. An

No.	Process Step	Potential Failure Modes	Potential Failure Effects	SEV	Potential (Root) Causes	OCC	Current Controls	DET	RPN	Recommended Corrective Action(s)	Action(s) Taken
1	Step 1	FM-1	Effect-1	4	C-1	8	CNTL-1 CNTL-2	2	64	CA-1 CA-2	CA-2
2	Step 1	FM-2	Effect-2	5	C-2	2	CNTL-3	7	70	CA-3	CA-3
3	Step 3	FM-3	Effect-2	8	C-3	1	CNTL-4	4	32	CA-4 CA-5	CA-4
4	Step 5	FM-4	Effect-3	2	C-4	4	CNTL-5 CNTL-6	5	40	CA-6	CA-6
5	Step 6	FM-5	Effect-4	5	C-5	2	CNTL-7	3	30	CA-7	CA-7

EXHIBIT 16.7 COMPLETED FMEA FORM

effective method of identifying and ultimately quantifying the operational risk in a company is through business process modeling (BPM) and simulation. For decades, simulation process modeling has been employed in manufacturing and transportation to model physical systems. Recently, this type of process modeling has been applied to business processes such as transaction processing and corporate governance processes. The process simulation model will aid the organization in:

- Developing insights into the operations of the business
- Leveraging assets and reducing costs
- Testing process changes before implementation (change management)
- Experimenting with process improvements to reduce cycle times and manage operational risk
- Conducting stress tests and scenario analysis

The speed of business today provides only short windows of opportunity. Businesses must bring new products and improvements to market quickly and cannot rely on lengthy, costly, or error-prone projects.

(e) APPLICATION: FRONT OFFICE SYSTEMS FOR A PROPRIETARY TRADING FIRM. The functions of a trading firm are generally classified into three areas: front, middle, and back offices. Each of the three areas can be considered a business process composed of multiple activities. The front office activities include the monitoring of real-time data feeds, the calculation engines or pricing analytics, order execution including the management of the trade orders, the manipulation of the trades in the queue, and real-time position monitoring. In addition to position selection and management, the front office is also responsible for some risk management activities. Some of the software used in the front office is off the shelf, but the calculation engines used to provide asset valuations are proprietary and homegrown software.

Trading firms will configure their front office systems differently depending on the level of automated trading versus trader-initiated trades, the types of products traded, and the analytical software used to analyze the data. Exhibit 16.8 is an illustration of the system interconnectivities in a typical front office. The desk traders have access to external information from CNN, Bloomberg, Reuters, exchange price and volume data, and internal valuations of financial assets based on real-time data from the exchanges. The data feeds are stored in a database and used by the trading applications and traders to determine what trades to place. Generally, the trades will go to a pay-per-look firm such as BATS, which operates as an electronic market maker. The pay-per-look firm has the opportunity to accept or reject the trades sent by the proprietary trader. If the first pay-per-look firm rejects the trade, it is sent to the next pay-per-look firm on the list. All of this transpires in milliseconds. The need for speed is essential to be competitive.

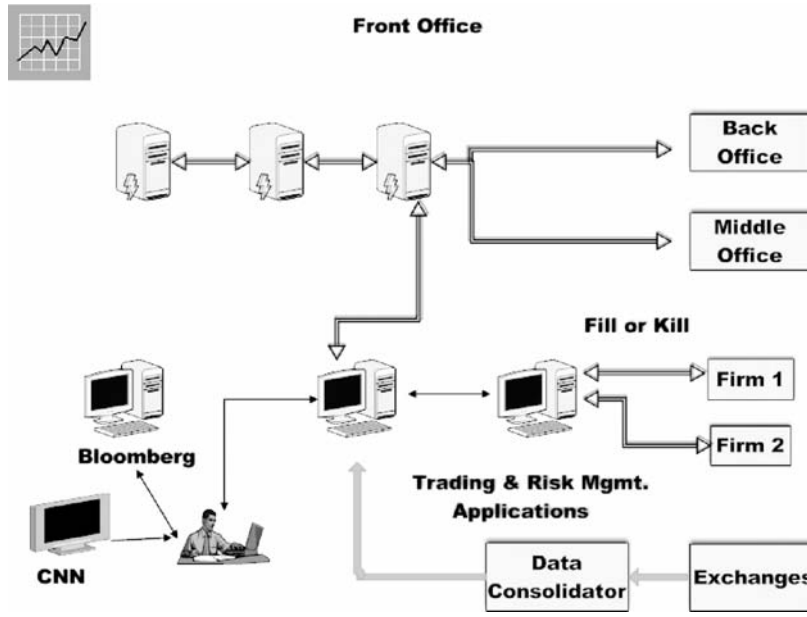


EXHIBIT 16.8 FRONT OFFICE CONFIGURATION

Trading firms must be able to manage, distribute, and process high volumes of data while simultaneously decreasing latency.[4]

In order to be competitive in the financial markets, trading firms rely on computing power, network sophistication, and quantitative research to drive the calculation engines of the system. Trading firms are constantly searching for an edge in the market, a new trading system, or a way to reduce their risk.

The risk profile of a proprietary trading desk or hedge fund is different from that of a brokerage firm. Proprietary trading firms have significant market risk from their portfolio positions. These firms aim to generate the highest return while retaining a certain risk profile. Consequently, risk monitoring is essential to maintaining the risk profile, including monitoring the position limits. For global trading firms, trading is generally performed in silos, which makes integrated risk management difficult. In fact, without an integrated view of risk, the trading firm may actually have a higher risk profile than is seen when the firm risk is viewed through silos.

(f) TRADING ROOM OPERATIONAL RISKS AND RISK MANAGEMENT. Unlike credit risk or market risk, operational risk is endogenous to the institution. It is linked to the nature and complexity of the activities, to the processes and systems in place, and to the quality of management and information flows. The lack of

appropriate controls and limitations can rapidly become disastrous for a trading firm, way beyond any capital requirements.

Trading room operational risks include but are not limited to:

- Human capital risk, such as inadequate staffing for required activities, lack of training, poor recruitment processes, and loss of key employees and knowledge capital. Trading firms are particularly vulnerable to rogue traders. Although most do not reach the level of notoriety of Nick Leeson, there are still many instances in the news of wayward traders.
- Modeling risk, including poor or inadequate models, poor back-testing procedures, and poor change management procedures.
- Software risk, which can take many forms, but in a trading environment spreadsheet errors are pervasive.
- Information technology (IT) infrastructure risk.
- Networking risk.
- Regulatory risk. Regulatory compliance and reporting (e.g., Sarbanes-Oxley and Basel II) require trading room technology be capable of real-time monitoring of transactions and risk exposures.

Operational risk management involves an array of methods and approaches that essentially serve two purposes: to reduce the dollar value of the average loss and to avoid catastrophic losses. Risk management is not new to trading firms. Before Basel I and II, IT departments implemented procedures to prevent security breaches and developed business continuity plans and disaster recovery plans.

(g) BUSINESS PROCESS MODEL FOR A TRADING ROOM. Real-time analytical trading applications are typically built with C++ and Java running in a Linux environment, because the speed of these applications and the entire trading platform is of critical importance. A millisecond or two late in processing real-time data can cause a firm to lose a trading opportunity. For this reason, over the past few years stream processing has become popular. Stream processing is a method of processing data in memory before the data are stored in a database. It achieves low-latency processing of high-volume real-time price and event data as well as historical data. Exhibit 16.9 illustrates the electronic trade-generation process without stream processing at a proprietary trading firm. Event data from QAI and real-time price data from a consolidator flow into a database. A Java trading algorithm taps into the database to determine if new trades should be placed, current positions need to be closed, or the portfolio needs to be rehedged. The trades generated by the trading algorithm are sent to pay-per-look firms.

The trading firm believes the introduction of a stream-processing program such as Streambase can reduce the processing time of the trade-generation system and give it an edge in the short run. The trading firm can estimate the reduction in latency by modeling the current and new designs with a BPM program.

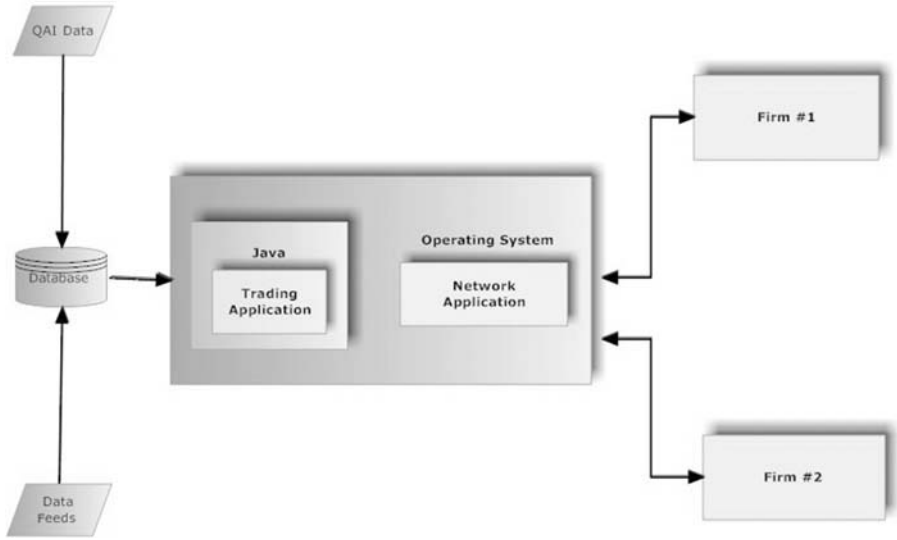


EXHIBIT 16.9 SIMPLIFIED ALGORITHMIC TRADING PROCESS

(h) EVALUATING SYSTEM CHANGES USING BUSINESS PROCESS MODELING SOFTWARE. Business process modeling (BPM) software allows a firm to assess the internal structures of the entire organization. The software enables the firm to separate processes, systems, and data into distinct layers, allowing the firm to monitor them independently. BPM software has the capability of modeling process performance, simulating scenarios, and stress testing the system. The proprietary trading firm interested in moving to stream processing can model the flow of data through the trade-generation process. The firm can model the volume of data coming into the system from the data consolidator and can model the time it takes for data to come in the door to the generation of a trade from the trading algorithm.

(i) CONCLUSION. Although BPM software has been around for several years, its application to operational risk is in its infancy. The software enables managers to be proactive in their approach to operational risk instead of reactive. What has been presented here is a simple example of the power of BPM.

16.6 QUANTIFY OPERATIONAL RISK

Statistical process control (SPC) is the name for many tools that aim to identify when processes become unstable. This type of quality control is most often associated with manufacturing environments but is very effective in general business process modeling. The most typical SPC is the control chart, which can take many forms. The cumulative sum (cusum) control chart is very effective in detecting small process shifts.

Business processes need to be stable and should operate with minor variability. Consider ABC Corporation, a company that is experiencing a rapid growth in sales. This growth affects many of the processes within the firm. Normally, vendor invoices have been paid within the standard 10-day period, allowing the company to capture prompt payment discounts. The fast growth in sales has slowed down the payment process and the firm has failed to capture the discounts, resulting in an increase in expenses.

Exhibit 16.10 shows the typical vendor payment process for ABC Corporation. Invoices flow into the accounting department from all the other departments within the firm. If the vendor is new to the firm, information about the vendor is put into a database. The invoice is governance reviewed (i.e., are the correct signature levels attached?). If the invoice fails the governance check, an e-mail is sent to the department submitting the invoice and the correct signatures are collected. Once the invoice passes the governance check, the invoice is approved for payment and placed in the queue for batch processing. The checks are printed and mailed once a week.

An increase in the volume of invoices due to rapid company growth can overload the system, leading to a delay in payments to the vendors and a loss

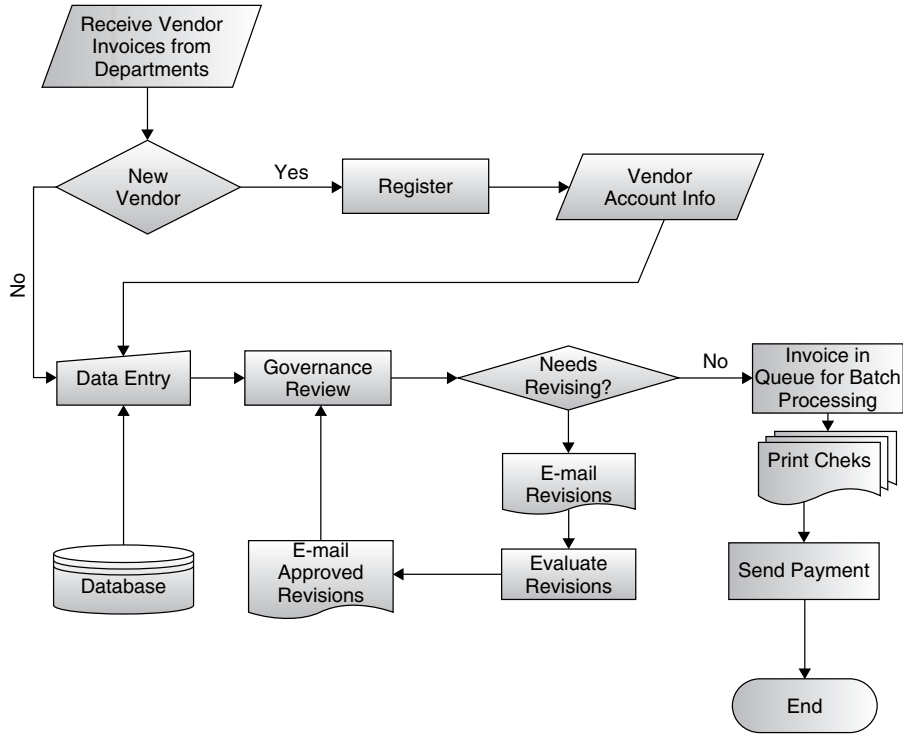


EXHIBIT 16.10 VENDOR PAYMENT PROCESS

Week	% Discount	Week	% Discount	Week	% Discount
1	95.00%	26	96.57%	51	86.50%
2	92.60%	27	97.98%	52	87.46%
3	94.94%	28	94.31%	53	75.19%
4	88.80%	29	92.82%	54	80.30%
5	97.05%	30	91.20%	55	86.22%
6	90.51%	31	97.26%	56	76.80%
7	97.46%	32	83.13%	57	78.19%
8	93.81%	33	80.74%	58	75.59%
9	90.49%	34	82.49%	59	75.42%
10	96.19%	35	86.19%	60	77.13%
11	88.17%	36	83.79%	61	77.85%
12	91.33%	37	88.85%	62	82.78%
13	90.55%	38	84.59%	63	80.53%
14	93.66%	39	82.51%	64	82.16%
15	96.27%	40	84.09%	65	77.60%
16	94.82%	41	83.52%	66	76.70%
17	94.51%	42	88.75%	67	79.52%
18	93.02%	43	82.03%	68	78.12%
19	94.52%	44	84.21%	69	84.23%
20	92.29%	45	82.34%	70	75.33%
21	92.05%	46	82.23%		
22	94.06%	47	79.97%		
23	90.73%	48	76.31%		
24	92.90%	49	82.75%		
25	96.85%	50	86.69%		

EXHIBIT 16.11 PERCENTAGE OF VENDOR DISCOUNTS RECEIVED

of the prompt payment discount. Exhibit 16.11 illustrates some of the weekly data ABC Corporation has collected over a 70-week period for the percentage of prompt payment discounts received.

During weeks 1 through 10, the percentage of vendor discounts received remained over 90 percent for all but one week. During weeks 60 through 70, after the growth spurt in sales began, the percentages dropped well below the 92 percent target level.

While there are many different flavors of cusum charts, ABC Corporation has decided to apply the tabular cusum to the vendor payment process. All cusum statistics incorporate all the information known about the process. The plain-vanilla cusum simply plots the cumulative sums of the deviations of the observed values and a target value.

$$C_i = \sum_{j=1}^{i} (x_j - \mu_0) \tag{1}$$

In equation (1), the cumulative sum at time i is found by summing all the deviations of the target value, μ_0, from the observed values, x_j. The target value is generally the process mean when the process is in control. For ABC Corporation, the target value will be set at 92 percent (i.e., 92 percent of the time ABC Corporation wants to capture the prompt payment discount).

The tabular cumulative sum (cusum) shown in Exhibit 16.12 is designed to identify when the mean of the process becomes unstable and sums the deviations above the target value with one statistic C^+ and the deviations below the target value with a second statistic C^-. The one-sided upper and lower cusums, C^+ and C^- are calculated as follows:

$$C_i^+ = \max[0, x_i - (\mu_0 - K) + C_{i-1}^+] \tag{2}$$

$$C_i^- = \max[0, (\mu_0 - K) - x_i + C_{i-1}^-] \tag{3}$$

The starting values for the upper and lower cusums are zero. In equations (2) and (3), K is called the slack value. It is chosen to be halfway between the target value, μ_0, and a point where the process is considered to be out of control. ABC Corporation's target value was set to 92 percent, and the slack value was chosen as 1 percent.

16.7 MONITOR AND CONTROL OPERATIONAL RISK

Operational risk is just one category of an organization's overall risk portfolio. After identifying, assessing, and quantifying risks, it is of utmost importance that there is a process in place to monitor and control or mitigate the residual risk that is present in any of the key processes. Instead of creating a separate process for monitoring and controlling operational risks, it is in the best interest of any organization to pull this process under the organization's overall risk monitoring and controlling strategy. The Basel Committee on Banking Supervision (BCBS) recommends that the board of directors should ensure that a bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained, and competent staff. BCBS also states that the internal audit function should not be directly responsible for operational risk management. Organizations should regularly review their risk control strategies to make sure they are effective and help organizations stay within their acceptable risk profiles.

16.8 CHANGE MANAGEMENT

Quantitative methods rely on accurate and timely data and process expertise to help in arriving at the right conclusions. Irrespective of the type of business being run, when implementing a new process or changing the way things are done, it is expected that there is always going to be some resistance from all or some part of the organization. It is very critical and essential that there is complete buy-in and

Week	% Discount	x– (Target + K)	C+	N+	(Target– K) – x	C–	N–
1	95.00%	0.02	0.02	1	–0.04	0	0
2	92.60%	0.00	0.00	0	–0.02	0.00	0
3	94.94%	0.02	0.02	1	–0.04	0.00	0
4	88.80%	–0.04	0.00	0	0.02	0.02	1
5	97.05%	0.04	0.04	1	–0.06	0.00	0
6	90.51%	–0.02	0.00	0	0.00	0.00	1
7	97.46%	0.04	0.04	1	–0.06	0.00	0
8	93.81%	0.01	0.05	2	–0.03	0.00	0
9	90.49%	–0.03	0.00	0	0.01	0.01	1
10	96.19%	0.03	0.03	1	–0.05	0.00	0
60	77.13%	–0.16	0.00	0	0.14	2.55	29
61	77.85%	–0.15	0.00	0	0.13	2.68	30
62	82.78%	–0.10	0.00	0	0.08	2.76	31
63	80.53%	–0.12	0.00	0	0.10	2.87	32
64	82.16%	–0.11	0.00	0	0.09	2.96	33
65	77.60%	–0.15	0.00	0	0.13	3.09	34
66	76.70%	–0.16	0.00	0	0.14	3.23	35
67	79.52%	–0.13	0.00	0	0.11	3.35	36
68	78.12%	–0.15	0.00	0	0.13	3.48	37
69	84.23%	–0.09	0.00	0	0.07	3.55	38
70	75.33%	–0.18	0.00	0	0.16	3.70	39

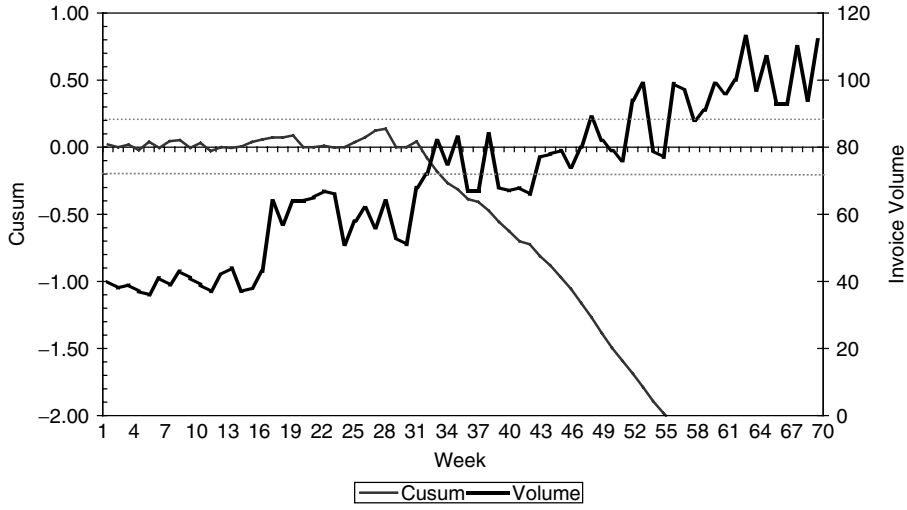


EXHIBIT 16.12 TABULAR CUMULATIVE SUM (CUSUM) CALCULATIONS

sponsorship from executive management and a top-down approach to managing operational risk. It is also very important that the process/functional owners have a clear understanding of the risk management strategy, support and take ownership in collecting all the necessary data, and actively participate in analyzing and taking appropriate actions as follow-up measures. In order to make this a reality, appropriate training should be provided to raise the general awareness of

quantitative methods/analysis and the resulting benefit to the organization as a whole. Appropriate metrics and proper incentives should be put in place for the employees of the organization to embrace this change.

Notes

1. Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk," February 2003.
2. Dee Harris and Tom Longstroth, "Moving Forward on the Loss Data Challenge," *OpRisk and Compliance* 7, no. 5 (2006).
3. COSO ERM Framework—www.coso.org/publications.htm.
4. Latency is commonly defined as the time it takes data to travel from the source to the destination.

References

Additional information on FMEA and six sigma tools can be found at www.isixsigma.com.

Basel Committee on Banking Supervision. 2003. "Sound Practices for the Management and Supervision of Operational Risk" (February).

COSO ERM framework—www.coso.org/publications.htm.

FMEA and six sigma training provided by the Quality Group, found at www.thequalitygroup.net.

Laguna, Manuel, and Johan Markland. 2005. *Business Process Modeling, Simulation, and Design.* Upper Saddle River, NJ: Pearson Prentice Hall.

CHAPTER 17

OPERATIONAL RISK MANAGEMENT IN FINANCIAL SERVICES

Anthony Tarantino, PhD

17.1 INTRODUCTION

Banking is at the forefront of the effort to quantify and measure operational risk and as such can be a role model beyond the financial services industry. The Basel Committee of the Bank for International Settlements (BIS) has created a new capital accord, known as Basel II. Basel II requires banks to establish an operational risk management (ORM) framework and compute an explicit capital charge for operational risk once it is adopted. Banks will need to be flexible and open to new approaches in managing operational risk.

Banks have historically defined operational risk as risk that did not fall into credit, market, or liquidity risk categories. Basel II has narrowed the definition somewhat as the loss, or risk of loss, resulting from inadequate or failed internal processes, people, or systems or from external events. This definition typically includes legal risk, but excludes strategic and reputational risk.

Most global banks will fall under the Basel II accord, which requires quantitative, qualitative, and modeling analysis of operational risk. The costs of meeting these requirements will typically run into several million dollars. While not all these banking requirements are applicable to other industries, they do provide a role model worth considering. All businesses face the challenge of balancing risks with opportunities and can easily quantify the monetary value of opportunities. Many fewer can quantify the monetary value of the operational risks.

The Basel Committee of BIS describes basic principles in improving operational risk management, which cover:

- Developing an appropriate risk management environment
- Risk management: identification, measurement, monitoring, and control
- Role of supervisors
- Role of disclosure[1]

Developing an Appropriate Risk Management Environment

- Board awareness and approval of the major aspects of operational risk and risk management as a distinct and controllable risk category
- Board approval and periodic review of operational risk strategy, which reflects the tolerance for risk categorization
- Management ownership and management of the board-approved operational risk strategy on an enterprise-wide level, including the applicable training, policies, procedures, and reward mechanisms
- The flow of information, which reinforces a robust operational risk culture at all levels of the organization

Risk Management: Identification, Measurement, Monitoring, and Control

- The identification of the inherent risks in all products, services, processes, and systems

- The risk-weighted review of new products, activities, and systems
- The establishment of the processes to measure, monitor, and mitigate operational risk at an enterprise level and down to the business units

ROLE OF SUPERVISORS

- Management assures systems are in place to identify, measure, monitor, and control operational risk
- Management assures the independent review and audit of the activities to control operational risk

ROLE OF DISCLOSURE

- The organization provides adequate disclosure to permit employees, shareholders, regulators, analysts, customers, and suppliers to assess their operational risk management and exposure.

(a) RATING AGENCY REQUIREMENTS. The rating agencies (Fitch, Moody's, and Standard & Poor's) have published several guidelines and standards promoting robust operational risk management. Their basic requirements typically include:

- An enterprise-wide risk identification process, which is independently reviewed and audited annually at a minimum
- A risk management committee and working groups with an enterprise-wide charter, which possesses the needed training, expertise, resources, and time to do its job
- The use of multiple risk metrics such stress testing, scenario analysis, benchmarks, option Greeks, value at risk (VaR), and so on
- Assurances that the risk committee and risk managers communicate on a regular basis beyond the reporting of risks
- A risk-weighted approval process for new products and strategies
- A risk reporting process that functions at all levels of the organization and includes all types of risks, including market, credit, liquidity, reputation, legal, and operational risk
- Clearly defined procedures, training, and enforcement around derivatives, hedging, and speculative strategies
- An ongoing independent review and audit process for all existing and proposed new risk management models
- An advocacy of risk diversification across the enterprise with the goal to avoid overconcentrations in any one area
- A centralized and dedicated risk management organization that is staffed with the appropriate subject matter experts and has the budget and charter to remain independent from those taking the risks

- A process and organization that identifies, communicates, and audits risk across the enterprise and includes correlations and interdependencies
- The use of multiple risk metrics, which includes both external and internal data, as well as both quantitative and qualitative techniques
- The assurance for the marking to market of all positions (i.e., the daily adjustment of an account to reflect accrued profits and losses and the corresponding asset accounting procedure that marks, or records, at their current market value and captures the delta between the current price and purchase price or book value)
- The creation, maintenance, and communication of policies and procedures to control derivatives, hedging, and modeling

The Basel II Committee provides a three-tiered categorization of operational risk (see Exhibit 17.1) that is applicable in many cases beyond the financial services industry.

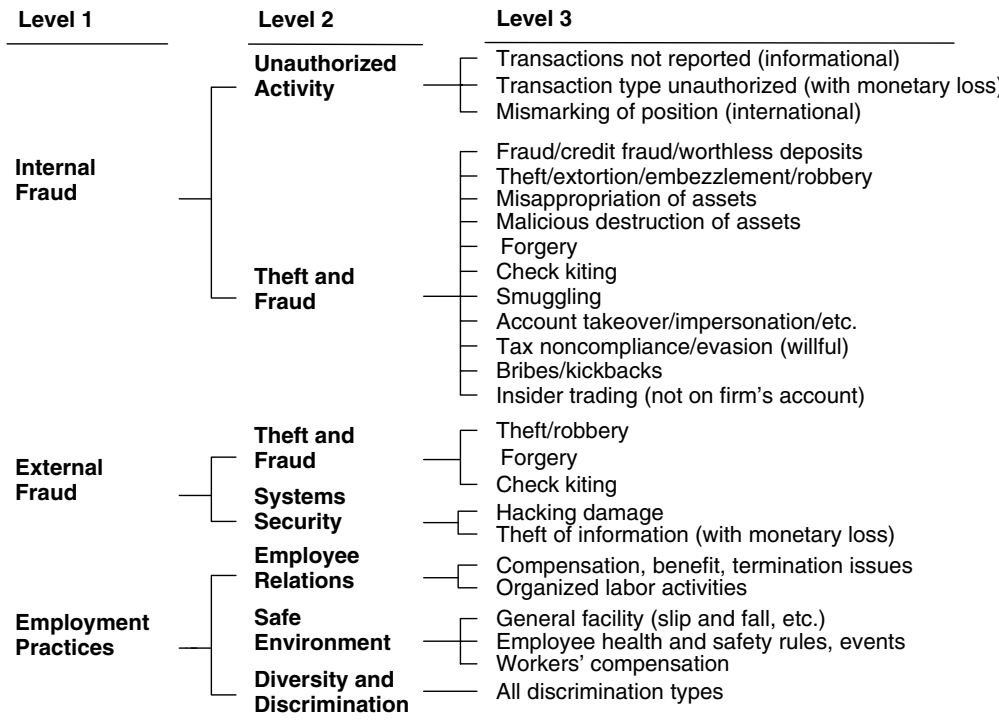


EXHIBIT 17.1 OPERATIONAL RISK LEVELS

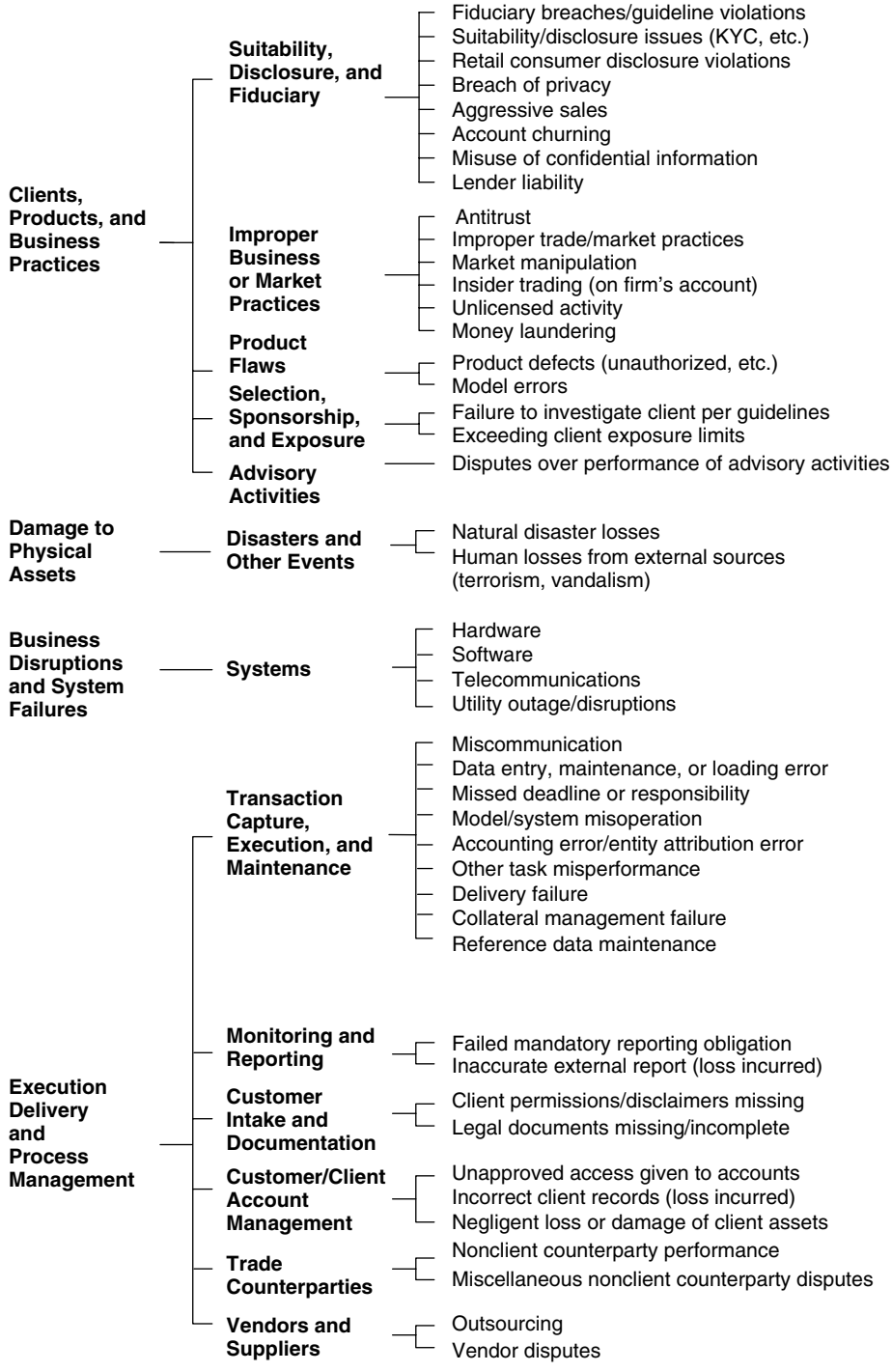


EXHIBIT 17.1 (*continued*) OPERATIONAL RISK LEVELS

17.2 APPROACHES TO OPERATIONAL RISK MANAGEMENT

Even banks and other financial services enterprises falling below the Basel II radar will come under pressure from rating agencies, analysts, and investors to adopt one of three major operational risk frameworks to calculate regulatory capital: The Basic Indicator Approach (BIA), The Standardized Approach (TSA), and the Advanced Measurement Approach (AMA). The BIA is designed for smaller banks, and Basel II banks are expected to at least begin with the TSA and then evolve to the AMA. The TSA and AMA will require a qualitative framework. There are substantial minimum capital requirements benefits in utilizing the AMA. So, even smaller organizations will find it difficult to compete without meeting the more demanding risk management regimes of the AMA.

(a) THE BASIC INDICATOR APPROACH (BIA). The BIA is the simplest of the three approaches, and will be the default option for most smaller banks. It applies a relatively straightforward calculation based on the bank's income to determine its capital requirements. Designed for smaller banks, the BIA does not require any entry-level criteria. It is expected to result in a higher capital charge and thus encourage the development more sophisticated and robust practices and methodologies. Under the BIA, a capital charge is calculated as a percentage of gross income. It will be an expensive proposition for most banks, offering few advantages over a flat capital charge. The United States has disqualified the BIA along with the TSA for its Basel II banks.

(b) THE STANDARDIZED APPROACH (TSA). Like the BIA, the TSA relies on calculations based on income, but with different percentages applying across different business lines. To take advantage of the standardized approach, firms will have to meet certain qualifying criteria. TSA requires the collection of internal loss data and will be used by many banks to transition into the AMA. Like the BIA, the capital charge under the TSA is a function of gross income, but it is calculated at a more detailed level—for eight business lines defined by the Basel II accords.

(c) THE ALTERNATE STANDARD APPROACH (ASA). The ASA permits banks to use loans and advances as the exposure indicator rather than the gross income indicator under TSA. Under the ASA, the operational risk capital charge is calculated in the same way as under the standardized approach, except in the case of retail and commercial banking. Banks, with the approval of the national regulator, can use loans and advances as the exposure indicator instead of the standardized approach's gross income indicator. The ASA is designed to support banks working in high-margin markets, such as emerging markets.

(d) THE ADVANCED MEASUREMENT APPROACH (AMA). The AMA is the most complex and expensive of the three options. Under the AMA, banks calculate their own capital requirements by developing and applying their own internal

risk measurement systems to estimate both expected losses (EL) and unexpected losses (UL). As with TSA, banks must meet certain qualifying criteria, and the risk measurement system will typically need to be validated by the appropriate national regulatory body. This is the most risk-sensitive approach with the objective of making the capital charge reflect the actual level of risk a bank faces. The Basel framework seeks a 99.9 percent capital confidence level in a one-year time frame. Banks seeking to use the AMA should strive to possess these characteristics:

- The bank's internal ORM system is tightly integrated into its day-to-day risk management processes; that is, it is not limited to determining regulatory capital but is part of a system aimed at improving operations and shareholder value and promoting stability.
- The bank reports on a regular basis its operational risk exposures, losses, and corrective actions.
- The bank has documented, published, trained, and certified its employees in its ORM systems.
- The bank regularly audits (internally and externally) its ORM systems to assure adherence to policies and procedures.
- The bank benchmarks its ORM systems against peers and best-in-class organizations. This includes a gap analysis and cost-versus-benefits analysis to close the gaps against the leaders.
- The bank can demonstrate that its ORM assumptions, processes, and technologies are adequate to meet its business and regulatory requirements. This includes validating the reliability, consistency, and thoroughness of its data inputs across the enterprise.
- The bank can demonstrate that its ORM system includes the following elements (described in greater detail later): internal and external loss data, risk control self-assessments (RCSA) scenario analysis, scorecards, key risk indicators.
- The bank publishes a risk profile report (detailed in the next section).

17.3 BANKING DOCUMENTATION

Banks should typically generate and evaluate the following reports in support of good operational risk management:

Risk Profile Report

- Earnings diagram (showing probability and distortion)
- Risk-weighted capital
- Economic capital
- Regulatory capital
- Main risk elements (identifying their size and current priority ratings)
- Internal fraud

- External fraud
- Employment practices and workplace safety
- Clients, products, and business practices
- Damage to physical assets
- Business disruption and systems failure
- Execution, delivery, and process management

Risk Profile Document

- Corporate governance, culture, and ethics
- Strategy, flexibility, and earnings stability
- Organization structure for risk management
- Systems and procedures (including existing and planned IT facilities)
- Contingency plans
- Fraud, corruption, and financial crime
- Audit and compliance
- Competency and key skills development
- Outsourcing (including insurance)
- Any other key issues impacting upon the risk profile of the bank

17.4 OPERATIONAL RISK TOOLS OVERVIEW

The collection and analysis of data are essential to gain an understanding of operational anticipated and actual losses. Quantitative analysis can be seen as a major advance, but is not a magic bullet by any means. Anyone who believes all operational risk can be quantified should consider 9/11. No operational risk management process could forecast the enormity of the human tragedy and its impact on an entire nation—far beyond the business centers of New York. Some organizations with robust data center resiliency failed because no one was left to operate the computers. The 2007 liquidity crisis in the United States, fostered by the meltdown of the subprime mortgage market, is a another example of failed risk management by some of the largest and most sophisticated organizations utilizing the most advanced technology, tools, and processes.

Quantitative analysis seeks to expose the underlying assumptions and tests empirical beliefs about the magnimity and criticality of losses. With this, it can provide enhanced accuracy and controls. Modeling is still evolving, with a number of mathematical models showing promise but limited by limitations in data. Although quantitative analysis will continue to grow in importance, qualitative analysis and controls should remain the backbone of good operational risk management.

Three main qualitative tools are emerging as a leading industry practice: risk control self-assessment (RCSA), scorecards, and key risk indicators (KRIs). Quantification tools use inputs from three main sources: internal data, external data, and scenarios.

(a) QUALITATIVE TOOL: RISK CONTROL SELF-ASSESSMENT (RCSA). The RCSA is used by many banks for the identification and evaluation of operational risk exposure. It is a logical first step and assumes the business owners and managers are closest to the issues and have the most expertise as to the source of the risk. The RCSA is a constructive process in compelling business owners to contemplate and then explain the issues at hand with the added benefit of increasing their accountability.

An RCSA is typically a bottom-up process by business managers, but may be a top-down process by senior stakeholders. This can provide a good blend—a granular view from the bottom up and an enterprise view from the top down. RCSA methods and tools include brainstorming sessions, interviews, facilitated workshops, scenario-building exercises, and questionnaires.

RCSA has its limitations in that it is subjective, and can be perverted by a corporate culture not willing to admit to mistakes or given to trying to shift blame. So executive management is vital in assuring RCSA participants that they will not suffer for speaking candidly and frankly.

(b) QUALITATIVE TOOL: SCORECARDS. Scorecards typically consist of generic questionnaires containing weighted risk-based questions with multiple-choice responses. They create qualitative assessments that can then be translated into quantitative measures such as a ranking of risks and in turn be used to adjust capital reserve levels. Unlike the Committee of Sponsoring Organizations (COSO) framework, there are rewards for internal control improvements—lower capital requirements with improvements in operational risk management.

Scorecards weigh responses with preset numerical values by their importance and can be used to spread capital charges across the appropriate business divisions and lines of business. Problems can arise due to the subjective nature of scorecards and manipulating the process to artificially lower capital charges.

(c) QUALITATIVE TOOL: KEY RISK INDICATORS. Key risk indicators (KRIs) are use to alert the organization to critical changes in risk, especially early warning alerts to changes in the control environment. Improving KRIs beyond after-the-fact loss indicators to truly predictive KRIs will be challenging, and KRIs cannot be expected to capture all potential losses.

(d) QUALITATIVE TOOL: SCENARIOS. Scenarios are a forward-looking process that can reflect risks for a given point of time. The scenario should mirror the bank's operational risk capital charges objective, which is designed to allocate capital against future losses. Scenarios are qualitative risk assessments in that they utilize expert opinion, but can be used to derive quantitative inputs into a capital model. There are four main steps in the scenario process:

1. Scenario generation
2. Scenario assessment

3. Review and validation of data quality
4. Incorporation of scenarios into the AMA process

An advanced measurement approach (AMA) has to cover all significant operational risks, and as such scenarios can be a useful tool. Scenarios can include both internal and external data, key risk factors, but can be vulnerable to subjective inputs. The rating agencies are very supportive of scenarios in the AMA and suggest they be updated as required to remain relevant to the current state environment.

(e) QUANTITATIVE TOOL: INTERNAL LOSS DATA. Internal loss data is key to any organization's efforts to improve ORM. The biggest issue most organizations face, though, is the lack of reliable and consistent operational risk data. It may seem surprising, but many banks only started accumulating internal loss data in order to prepare for Basel II. Basel II requires a minimum of three years' worth of data to start and five years' worth of data on an ongoing basis as part of the AMA.

The quality of internal loss data will be a factor and must be available across all business lines and geographies. Ideally, it should also include near-loss data. It will be critical to capture all economic losses, not just major or material losses with a large impact on the bottom line. This is especially important in predicting expected losses (ELs) even though they typically represent less than 25 percent of all losses.[2]

Many loss events result from a variety and combination of factors, which makes their classification difficult. In theory, the same loss event could fall into credit, market, and operational risk buckets. There is also an issue as to the organization's acceptance of risk. Many organizations are hesitant to capture operational risk losses as a negative reflection on their performance, but view market and credit risks as a cost of doing business and therefore more acceptable.

One way to resolve these issues is for the organization to reconcile the general ledger with operational loss data. This will work for accounting losses but will not capture lost opportunity costs. Few banks have bought into this as a solution, arguing that costs outweigh the benefits.[3] It difficult to see how operational loss data can be accepted by external auditors, regulators, and analysts over the long term if there is no tie to the general ledger.

Another method of validating internal loss data is to compare it with peer organizations via externally available data and then scale the data to reflect the organization's environment.

(f) QUANTITATIVE TOOL: EXTERNAL DATA. External data is needed for the simple reason that there is typically a lack of internal data, especially data around unexpected losses, which represent the large majority of losses in most banks. Issues in the use of external data stem from its sources—data providers or bank consortia. External data must be mapped, scaled, and adapted to each bank's business, legal, regulatory, technical, control, and cultural environment.

17.5 U.S. NPR: AMA APPROACHES FOR OPERATIONAL RISK[4]

(a) BACKGROUND. The Federal Reserve Board issued its latest Draft Notice of Proposed Rulemaking (NPR) on February 15, 2007, for a U.S. risk-based capital framework based on the Basel II accord. The initial NPR was issued in August 2003, and both the Office of Thrift Supervision and Office of the Comptroller of the Currency approve each NPR before it is published for comment. Congress and regulators approved the NPR in July, 2007.

The majority of changes constitute minor clarifications and local adaptations of the Basel II rules. There are no special adjustments for small and medium-sized enterprises (SMEs) in the NPR, since no compelling evidence was found to support a favorable capital treatment.

Only the advanced approaches to credit risk (A-IRB) and operational risk (AMA) are permitted under the U.S. NPR. Key points in the NPR:

- The capital-adequacy framework of Basel II is intended to produce more sensitive, risk-based capital requirements than the existing general risk-based capital rules resulting from Basel I.
- The proposed rule maintains the general risk-based capital rules' minimum tier-1, risk-based capital ratio of 4 percent and total risk-based capital ratio of 8 percent.
- The primary difference between the proposed rule and the existing rules is the methodology used for calculating the ratio's denominator—risk-weighted assets.
- Banks applying the new rule would rely on internal risk measurement systems to estimate risk parameters for exposures.
- The banks would use specific risk-based capital formulas to transform the internally calculated risk parameters into risk-weighted asset amounts for general credit risk (including wholesale and retail exposures), securitization, and equity exposures.
- The proposed rule requires that a bank's systems and processes used for risk-based capital purposes be sufficiently consistent with its existing internal risk.
- The Advanced Notice of Proposed Rule Making (ANPR) only proposed the advanced Basel II approaches, which the agencies believed most appropriate for large, internationally active U.S. banks.
- This NPR addresses only credit and operational risk.

NPR Scope. The proposal identifies three groups of banks:

1. Banks required to adopt the advanced approach (core banks)
2. Banks that voluntarily adopt advanced approaches (opt-in banks)
3. Banks that do not adopt the advanced approaches (general banks)

A bank would be considered a core bank if its consolidated total assets are $250 billion or more, consolidated on-balance-sheet foreign exposure is $10

billion or more, or it is a subsidiary of another depository institution or bank holding company using the advanced approach. A bank holding company would be a core bank if its consolidated total assets (excluding assets held by an insurance underwriting subsidiary) are $250 billion or more, consolidated on-balance-sheet foreign exposure is $10 billion or more, or it has a subsidiary depository institution using the advanced approach.

NPR Timing. Before moving to the advanced approach for risk-based capital purposes, a bank would have to complete a satisfactory parallel run of at least four consecutive quarters, during which the bank's primary regulator deems the bank's compliance with the qualification requirements as satisfactory. Under the new proposal, the first opportunity for a bank to begin a parallel run would be January 2008 (a delay of one year relative to the Basel II accord). During the parallel run, a bank would remain subject to the existing general risk-based capital rules, but would also calculate and report its capital ratios to its primary federal regulator. The proposed U.S. ruling would also impose a longer, more gradual transition period than that of the Basel II accord.

NPR's Treatment of the Advanced Approach. A bank's advanced approach systems would have to incorporate a framework of five interdependent components to evaluate credit and operation risk, and measure regulatory capital:

- A risk-rating and segmentation system that assigns ratings to individual wholesale obligors and exposures and assigns individual retail exposures to segments
- A quantification process that translates the risk characteristics of wholesale obligors and exposures, and segments of retail exposures into numerical risk parameters used as inputs to the internal ratings-based, risk-based formulas
- An ongoing process that validates the accuracy of the rating assignments, segmentation, and risk parameters
- A data management and maintenance system that supports the advanced approach systems
- Oversight and control mechanisms that ensure the advanced approach systems are functioning effectively and producing accurate results

NPR's Review and Approval of the Advanced Approach. Under the proposal, bank senior management would be responsible for ensuring that all system components used under the advanced approaches function effectively and are in compliance with the advanced approach qualification requirements. The bank's board (or designated committee) would evaluate and approve, at least annually, the effectiveness of the bank's advanced (risk-based capital measurement) systems. A bank would be required to independently validate its advanced systems on an ongoing basis. Validation would include three components:

1. Evaluation of the soundness of advanced systems' ongoing monitoring, including verifying processes and comparing the bank's internal estimates

with relevant internal and external data sources, or results using other techniques such as benchmarking
2. Analysis of outcomes, including comparisons of actual outcomes to the bank's internal estimates, using back-testing or similar methods
3. An internal audit function, independent of business-line management, to assess, at least annually, the effectiveness of controls supporting the bank's advanced systems

The NPR's treatment of the AMA and operational risk can be summarized:

- Banks would have to periodically stress-test their advanced systems to ensure they remain at least adequately capitalized during all phases of the economic cycle, including downturns.
- Banks would be required to document all material aspects of their advanced systems, including internal risk-rating and segmentation systems, risk-parameter quantification systems, model design, assumptions, and validation results.
- Operational risk components of the new proposal do not materially deviate from those required by the Basel II accord. The assessment of operational risk includes internal and external operational loss event data, results of scenario analysis, and assessments of the bank's business environment and internal control.
- Public disclosures required would include capital structure, capital adequacy, credit risk, securitization, operational risk, equities, and interest-rate risk in nontrading activities.

Before a bank may use the advanced approaches for risk-based capital purposes, it must understand these points:

- A bank's primary federal supervisor would be responsible for evaluating the bank's initial and ongoing compliance with the qualification requirements for the advanced approaches.
- During implementation of the advanced approaches:
    - A bank would work closely with its primary federal supervisor to ensure that its risk measurement and management systems are fully functional and reliable and are able to generate risk parameter estimates that can be used to calculate the risk-based capital ratios correctly under the advanced approaches.
    - The implementation plan, including the gap analysis and action plan, will provide a basis for ongoing supervisory dialogue and review during this period.
    - The primary federal supervisor will assess a bank's progress relative to its implementation plan. To the extent that adjustments to target

dates are needed, these adjustments would be made subject to the ongoing supervisory discussion between the bank and its primary federal supervisor.

- The Internal Rating Based Approach (IRB) Guidance supplements the NPR and provides additional context and detail to help banks meet the qualification requirements in the NPR relevant to a bank's systems and processes for credit risk. Thus, the guidance should be read alongside the NPR to obtain a full perspective of the underlying requirements in the proposed rule.
- The guidance does not contain additional proposed requirements that are not in the NPR.
- Chapters 5, 9, 10, and 11 are being issued for the first time and supplement the detailed discussion of those topics in the NPR. Similar to the previously proposed corporate and retail guidance, the IRB Guidance contains supervisory standards (designated with an "S") that highlight important elements of a bank's advanced systems for credit risk.
- The supervisory standards contained in the previously proposed corporate and retail guidance documents have been consolidated and updated and new supervisory standards are proposed.

Some of the specific revisions to the AMA Guidance include:

- Clarifying the roles of a bank's board of directors and management in developing and overseeing the implementation of the bank's AMA framework
- Expanding Standard 5 to address the integration of the bank's operational risk management, data and assessment, and quantification processes into the bank's existing risk management decision-making processes
- Expanding and clarifying operational risk quantification standards both to reflect the evolution of industry practices, as well as to address supervisory concerns
- Clarifying supervisory expectations regarding the use of scenario analysis, the key elements used to support operational risk management and measurement, and eligible operational risk offsets (see Standards 20, 24, and 26, respectively)
- Adding Standard 25, which discusses how frequently a bank must recalculate its estimate of operational risk exposure and its risk-based capital requirement for operational risk
- Adding Standard 27 that a bank must employ a unit of measure that is appropriate for its range of business activities and the variety of operational loss events to which it is exposed
- Expanding the discussion on dependence modeling in Standard 28

- Adding a section that discusses a bank's use, in certain limited circumstances, of an alternative quantification system to estimate its operational risk exposure

What follows is a summary of the February 15, 2007 NPR that impacts operational risk.

(b) OPERATIONAL RISK MANAGEMENT

(i) Governance. **S 1.** The bank's AMA System must include an operational risk management function and audit function that are independent of business line management. The operational risk management function should address operational risk on a firmwide basis.

S 2. The bank must have and document a process that clearly describes its AMA system, including how the bank identifies, measures, monitors, and controls operational risk.

S 3. The bank must maintain effective internal controls supporting its AMA system. As one of the foundations of safe and sound banking, sound internal controls are essential to a bank's management of operational risk and are an important requirement for AMA qualification.

(ii) Board of Directors and Management Oversight. **S 4.** The bank must ensure that an effective framework is in place to identify, measure, monitor, and control operational risk, and to accurately compute the bank's operational risk component of the bank's risk-based capital requirement. The board of directors must at least annually evaluate the effectiveness of, and approve, the bank's AMA system, including the strength of the bank's control infrastructure.

S 5. The board of directors and management should ensure that the bank's operational risk management, data and assessment, and quantification processes are appropriately integrated into the bank's existing risk management and decision-making processes and that there are adequate resources to support these processes throughout the bank. A strong board of directors and management oversight form the cornerstone of an effective operational risk management process. The board of directors is responsible for overseeing the establishment and ongoing effectiveness of the AMA system. The board of directors must approve the bank's written implementation plan. In addition, the board of directors must at least annually evaluate the effectiveness of, and approve, the bank's AMA system.

(iii) Firmwide Operational Risk Management Function. **S 6.** The bank must have a firmwide operational risk management function that oversees the AMA system and is independent of business line management. The operational risk management function is also responsible for the development of operational risk

data and assessment systems, operational risk quantification systems, and related processes throughout the bank.

S 7. The firmwide operational risk management function should ensure adequate analysis and reporting of operational risk information. The function should also develop and report on the firmwide operational risk profile. The roles and responsibilities of the firmwide operational risk management function may vary among banks, but should be clearly documented in operational risk policies and procedures. The firmwide function should have organizational stature commensurate with the bank's operational risk profile. At a minimum, the function should ensure the development of policies, processes, and procedures that explicitly manage operational risk as a distinct risk.

(iv) Line of Business Management. **S 8.** Line of business management is responsible for ensuring appropriate day-to-day management of the operational risks within its business unit.

S 9. Line of business management should ensure that internal controls and practices within its business unit are consistent with firmwide policies, processes, and procedures. Line of business management should ensure that business-specific policies, processes, and procedures are in place, and appropriate staff is available to manage operational risk associated with the products and activities offered. Implementation of the AMA system within each line of business should correspond to the scope of that business and its operational complexity and risk profile. Line of business operational risk reporting should be appropriate in frequency and scope to identify, measure, monitor, and control operational risk. Reporting should also address the condition of the internal control environment for a given line of business.

(v) Reporting. **S 10.** The board of directors and senior management must receive reports on operational risk exposure, operational risk loss events, and other relevant operational risk information. The reports should include information regarding firmwide and business line risk profiles, loss experience, and relevant business environment and internal control factor assessments. These reports should be received quarterly. To facilitate monitoring of operational risk, results from the data and assessment, and quantification processes should be summarized and included in reports that can be used by different audiences to understand, manage, and control operational risk and losses. Reports generated by the bank's AMA system should provide the foundation for reporting to the board of directors and senior management. Comprehensive management reporting, geared toward the firmwide operational risk management function and line of business management, should include:

- Operational loss experience, including an overview and assessment of loss experience over time
- Operational risk exposure

- Changes in assessments of business environment and internal control factors
- Changes in factors signaling an increased risk of future losses
- Trend analysis, allowing line of business and independent firmwide operational risk management to assess and manage operational risk exposures, systemic line of business risk issues, and other corporate risk issues
- Policy and risk tolerance reporting
- Operational risk causal factors

(c) OPERATIONAL RISK DATA AND ASSESSMENT. The bank must have operational risk data and assessment systems that include credible, transparent, systematic, and verifiable processes that incorporate the following elements on an ongoing basis:

- Internal operational loss event data
- Relevant external operational loss event data
- Scenario analysis
- Assessments of the bank's business environment and internal control factors

In addition, the operational risk data and assessment systems must be structured in a manner consistent with the bank's current business activities, risk profile, technological processes, and risk management processes. The operational risk data and assessment systems should provide for the consistent and comprehensive capture of the four elements needed to measure and verify the bank's operational risk exposure. The four elements should be combined in a manner that most effectively allows the bank to quantify its exposure to operational risk.

(i) Capture and Maintenance of Elements. **S 11.** The bank must have a systematic process for incorporating internal loss event data, external loss event data, scenario analyses, and assessments of its business environment and internal controls factors to support both its operational risk management and measurement framework, as well as its calculation of the bank's operational risk component of its risk-based capital requirement.

S 12. The bank must use the regulatory definition of operational risk when assessing the operational risks to which the bank is exposed in order to calculate its risk-based capital requirement for operational risk. The bank should have clear standards for the collection and modification of all four elements in the operational risk data and assessment systems that support its AMA system.

(ii) Internal Operational Loss Event Data. **S 13.** The bank must have a historical observation period of at least five years for internal operational loss event data. A shorter period may be approved by the primary federal supervisor to address transitional situations, such as integrating a new business line. Internal data should be captured across all business lines, corporate functions, events,

product types, and geographic locations. The bank must have a systematic process for capturing and using internal operational loss event data in its operational risk data and assessment systems.

S 14. The bank should be able to map internal operational losses to the seven operational loss event categories.

S 15. The bank should have a policy that identifies when an operational loss is recognized and should be added to the loss event database. The policy should provide for consistent treatment across the bank.

S 16. The bank may establish appropriate internal operational loss event data thresholds and, if so, must demonstrate the appropriateness of such thresholds.

S 17. The bank should have a clear policy that allows for the consistent treatment of loss event classifications (for example, credit, market, or operational loss events) across the organization. Internal data with sufficient integrity is important in identifying the level of and trends in operational risk. A key to internal data integrity is the consistent and complete capture of loss event data across the bank. The bank must have a minimum historical observation period of five years of internal operational loss event data, or such shorter transitional period approved by the bank's primary federal supervisor. The description of the loss event, including causal factors, should be collected for internal operational loss events. Examples of additional loss event information to be collected include:

- Gross loss amount
- Where the loss is reported and expensed
- Loss event type category
- Date of the loss
- Discovery date of the loss
- Event end date
- Insurance recoveries
- Other recoveries
- Adjustments to the loss estimate

(iii) External Operational Loss Event Data. **S 18.** The bank must have a systematic process for determining how external loss data will be incorporated into its operational risk data and assessment systems.

S 19. The bank should systematically review external data to ensure an understanding of industry operational loss experience. External data may serve a number of different purposes in an AMA system. For example, where internal loss data are limited, external data may be a useful input in determining the bank's level of operational risk exposure. Even where external loss data are not an explicit input to a bank's database, such data may provide a means for the bank to understand industry experience and assess the adequacy of its internal data. External data may also prove useful to inform scenario analysis, provide additional data for severity distributions, or in model validation and out-of-sample testing.

The bank must establish a systematic process for determining the methodologies for incorporating external loss data into its operational risk data and assessment systems. To incorporate external loss data into a bank's framework, examples of the type of information a bank should collect include:

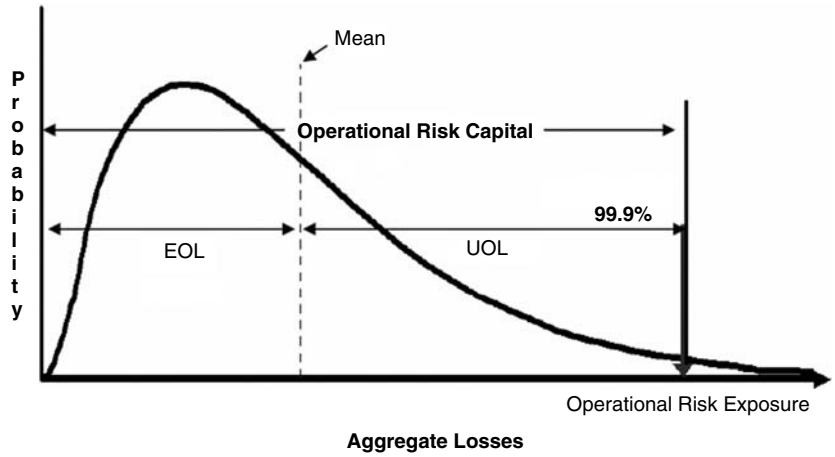
- Loss amount
- Loss description
- Loss event type category
- Loss event date
- Adjustments to the loss amount (for example, recoveries and insurance settlements) to the extent that they are known
- Sufficient information about the reporting institution to facilitate comparison to its own organization

(iv) Scenario Analysis. **S 20.** The bank must have a systematic process for determining how scenario analysis will be incorporated into its operational risk data and assessment systems. Scenario analysis allows the bank to incorporate forward-looking elements into its operational risk data and assessment systems. More specifically, scenario analysis is a systematic process of obtaining expert opinions from business and risk managers to derive reasoned assessments of the likelihood and loss impact of plausible high-severity operational losses that may occur at a bank. Scenario analysis is especially relevant for business lines or operational loss event types in which internal data, external data, or assessments of business environment and internal control factors do not provide a sufficiently robust estimate of the bank's exposure to operational risk. For example, a bank's scenario analysis should include consideration of high-severity loss events that occur infrequently in the industry. It could also include the effects of mergers or other significant organizational changes that may affect the nature of operational losses in the future. Business line and risk management experts' use of well-reasoned, external data may itself be a form of scenario analysis.

(v) Business Environment and Internal Control Factors. **S 21.** The bank must incorporate business environment and internal control factors into the bank's operational risk data and assessment systems.

S 22. The bank must periodically compare the results of its business environment and internal control factor assessments against the bank's actual operational risk loss experience. Business environment and internal control factors are indicators of the bank's operational risk profile that reflect the underlying business risk factors, an assessment of the current internal control environment, and a forward-looking assessment of the bank's control environment.

(d) OPERATIONAL RISK QUANTIFICATION. A bank must have a comprehensive operational risk quantification system, using inputs from its data and



Note: Graph is a stylized representation of operational risk quantification and does not incorporate the concepts of eligible operational loss offsets or qualifying risk mitigants that a bank may be able to consider in the calculation of its risk-based capital requirement for operational risk.

EXHIBIT 17.2 STYLIZED REPRESENTATION OF RISK QUANTIFICATION

assessment systems, that provides an estimate of the bank's operational risk exposure, which is defined as the 99.9th percentile of the distribution of potential aggregate operational losses over a one-year horizon. The bank's operational risk exposure is the starting point in determining the risk-based capital requirement for operational risk. (See Exhibit 17.2.)

A bank's estimate of operational risk exposure includes both expected operational loss (EOL) and unexpected operational loss (UOL), forming the basis of the bank's risk-based capital requirement for operational risk. The bank's estimate of operational risk exposure should also consider qualitative factors (for example, changes in business environment and internal control factors). Qualitative factors can be incorporated into the bank's quantification methodology in different ways and at different modeling stages. While not prescribing a specific methodology, the agencies will assess the processes banks use to integrate qualitative factors into the quantification of operational risk exposure.

Operational risk exposure may be reduced with eligible operational risk offsets, up to the amount of EOL. The bank's primary federal supervisor will review the bank's use of eligible operational risk offsets for appropriateness. A bank may also adjust its operational risk exposure to reflect reductions from operational risk mitigates (for example, insurance), subject to the qualification requirements and limits.

The dollar risk-based capital requirement for operational risk, resulting from the bank's risk quantification system, is the greater of:

- The bank's operational risk exposure adjusted for qualifying operational risk mitigants minus eligible operational risk offsets
- 0.8 multiplied by the difference between the bank's operational risk exposure and eligible operational risk offsets (if any)

If the bank has no qualifying operational risk mitigants, the dollar risk-based capital requirement for operational risk is equal to its operational risk exposure less any eligible operational risk offsets.

In recognition of the modeling challenges in legal entities with little internal operational risk loss data, a bank may generate an estimate of its operational risk exposure using an alternative approach to that described earlier, with the prior written approval of its primary federal supervisor.

The bank's risk-weighted asset amount for operational risk equals the bank's dollar risk-based capital requirement for operational risk determined as described earlier multiplied by 12.5.

(i) Analytical Framework. **S 23.** The bank must have an operational risk quantification system that provides an estimate of the bank's operational risk exposure.

S 24. The bank's operational risk quantification system must use a combination of internal operational loss event data, relevant external operational loss event data, business environment and internal control factor assessments, and scenario analysis results. The bank should combine these elements in a manner that most effectively enables it to quantify its operational risk exposure. The bank should choose the analytical framework that is most appropriate to its business model.

S 25. The bank must review and update its operational risk quantification system whenever it becomes aware of information that may have a material effect on the bank's estimate of operational risk exposure or risk-based capital requirement for operational risk, but no less frequently than annually. A complete review and recalculation of the bank's quantification system, including all modeling inputs and assumptions, must be done at least annually.

(ii) Eligible Operational Risk Offsets. **S 26.** In calculating the risk-based capital requirement for operational risk, management may deduct certain eligible operational risk offsets from its estimate of operational risk exposure. To the extent that these offsets do not fully cover expected operational loss (EOL), the bank's risk-based capital requirement for operational risk must incorporate the shortfall. Eligible operational risk offsets may be used to offset only EOL, not UOL, and are measured and accounted for, including how they meet the conditions outlined earlier.

(iii) Unit of Measure. **S 27.** The bank must employ a unit of measure that is appropriate for the bank's range of business activities and the variety of operational loss events to which it is exposed, and that does not combine business activities or operational loss events with different risk profiles within the same loss distribution. Banks should weigh the advantages and disadvantages of estimating a single loss distribution or very few loss distributions (top-down approach), versus a larger number of loss distributions for specific event types and/or business lines (bottom-up approach). One advantage of the top-down approach is that data sufficiency is less likely to be a limiting factor, whereas with the bottom-up approach there may be pockets of missing or limited data. However, a loss severity distribution may be more difficult to specify with the top-down approach, as it is a statistical mixture of (potentially) heterogeneous business line and event type distributions. Supervisors will consider the conditions necessary for the validity of top-down approaches and evaluate whether these conditions are met in their particular individual circumstances.

(iv) Accounting for Dependence. **S 28.** The bank may use internal estimates of dependence among operational losses within and across business lines and operational loss events if the bank can demonstrate to the satisfaction of its primary federal supervisor that the bank's process for estimating dependence is sound, robust to a variety of scenarios, and implemented with integrity, and allows for uncertainty surrounding the estimates. If the bank has not made such a demonstration, it must sum operational risk exposure estimates across units of measures to calculate its total operational risk exposure. A bank using internal estimates of dependence, whether explicit or embedded, must demonstrate that its process for estimating dependency is sound, robust to a variety of scenarios, and implemented with integrity, and allows for the uncertainty surrounding the estimates.

(v) Risk Mitigation. **S 29.** The bank may adjust its operational risk exposure results by no more than 20 percent to reflect the impact of operational risk mitigants. In order to recognize the effects of risk mitigants, management must estimate its operational risk exposure with and without their effects. There are many mechanisms to manage operational risk, including risk transfer through risk mitigation products. Because risk mitigation can be an important element in limiting or reducing operational risk exposure in a bank, an adjustment that will directly affect the amount of regulatory capital that is held for operational risk is being permitted. The adjustment is limited to 20 percent of the overall operational risk exposure less any eligible operational risk offsets. In order to recognize the effects of risk mitigants, the bank must calculate two estimates of its operational risk exposure. The first estimate should include the effects of risk mitigants, in addition to all other adjustments and effects (for example, expected losses, diversification, and qualitative adjustments) that are to be reflected in the risk-based capital requirement for operational risk. The second estimate should be identical to the first, except that it should not reflect the effects of risk mitigants.

(vi) Alternative Approaches for Depository Institutions. The agencies recognize that in certain limited circumstances, there may not be sufficient data available for a bank to generate an AMA estimate of its own operational risk exposure at the 99.9 percent confidence level. In these circumstances, a bank may propose use of an alternative operational risk quantification system, subject to approval by the bank's primary federal supervisor. The agencies are not prescribing any estimation methodologies for the alternative approach. However, the agencies expect that use of an alternative approach will occur on a very limited basis. Furthermore, such approaches will not be available at the bank holding company level.

(vii) Documentation of Operational Risk Quantification Systems. **S 30.** The bank must document all material aspects of its AMA system. This documentation should include the rationale for the development, operation, and assumptions underpinning its chosen analytical framework, including the choice of inputs, distributional assumptions, and the weighting across qualitative and quantitative elements.

Whatever analytical approach a bank chooses, it must document all material aspects of its AMA system. Generally, the documentation should include a discussion of the bank's modeling philosophy, a how-to guide that would provide sufficient detail for an independent party to substantially replicate the capital calculation, and an audit trail of any changes to the framework's assumptions. More specifically, this documentation should:

- Provide an overview of the analytical approach (for example, description of the model(s) and/or statistical technique(s) used, model inputs and outputs, and steps taken to ensure the integrity of the data used in the estimation process).
- Identify how the different inputs are combined and weighted to arrive at the overall operational risk exposure so that the analytical framework is transparent.
- Demonstrate that the analytical framework is comprehensive and internally consistent. Comprehensive and consistent means that all required inputs are incorporated and appropriately weighted and that there are not overlaps or double counting.
- Identify the quantitative assumptions embedded in the methodology and provide explanations for the choice and limitations of these assumptions (for example, quantitative assumptions include distributional assumptions, as well as dependence assumptions between operational losses across and within business lines).
- Include, where possible, documentation of quantitative measures of each assumption's validity, based on the relevant data elements (for example, statistical goodness-of-fit tests should be used to evaluate distributional assumptions).
- Identify the qualitative assumptions embedded in the methodology and provide explanations for the choice of these assumptions. (For example,

qualitative assumptions could include the use of business environment and internal control factor assessments, scenario analysis, and business judgment to derive dependence assumptions.)

- Provide results based on alternative quantitative and qualitative assumptions to gauge the overall model's sensitivity to these assumptions.
- Identify all simplifying or normalizing assumptions. (For example, assumptions could include setting a maximum cap on losses in order to influence the shape of the severity distribution or to normalize results at specific units of measure for internal capital purposes or prior to aggregation. Assumptions should be consistent with relevant loss data from both internal and external sources).
- Provide results to assess the impact of simplifying or normalizing assumptions.
- Compare the operational risk exposure estimate generated by the analytical framework with actual loss experience over time, to assess the framework's performance and the reasonableness of its outputs.
- Identify all limitations of and changes to assumptions, and provide explanations for such changes.
- Include details and rationale for establishing thresholds and their use.
- Include information on the technical process underlying the analytical approach (for example, programming language(s) and software used, logical process flow diagrams, system or source of record for the data elements, and how outputs are used in subsequent steps of the approach).
- Include technical change control information relating to the analytical approach (for example, a record of the changes, the associated rationale for the changes, and the effects on the analytical approach).
- Provide the results of an independent verification and validation of the analytical framework.

Notes

1. Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk," February 2003.
2. Fitch Ratings, "Bank Operational Risk Assessment Methodology," *Criteria Report*, July 13, 2005.
3. Ibid.
4. Department of the Treasury, Office of the Comptroller of the Currency [Docket No. OCC-2007-004], Federal Reserve System [Docket No. OP-1277], Federal Deposit Insurance Corporation, Department of the Treasury, Office of Thrift Supervision [No. 2007-06], "Proposed Supervisory Guidance for Internal Ratings-Based Systems for Credit Risk, Advanced Measurement Approaches for Operational Risk, and the Supervisory Review Process (Pillar 2) Related to Basel II Implementation," February 15, 2007.

PART 4

TECHNOLOGY AND TOOLS

CHAPTER 18

WHAT TO LOOK FOR IN ENTERPRISE CONTENT MANAGEMENT FOR COMPLIANCE

Julia Koo

Enterprise content management (ECM) systems are important compliance investments because they reduce the risk of corporate scandals around discovery, alteration, or inappropriate destruction of documents and e-mails. These scandals are results of proliferation of poorly managed unstructured data (content). ECM's components, including content management, document management, record management, and process management, help to eliminate process gaps that make these scandals possible. This chapter discusses standard, advanced, and next generation compliance-related requirements of ECM systems.

18.1 INTRODUCTION

Due to rapid and accelerating explosion of all types of content, including documents, e-mails, instant massages, images, and the like, the need for creating an enterprise-wide content management system becomes crucial. ECM can ensure security and provide a full audit trail in content change, access, and destruction. This facilitates discovery and manages the proliferation of sensitive content. As a result, better ECM helps companies to better address the risk of noncompliance with regulations.

18.2 FINANCIAL COMPLIANCE PROCESS

The financial compliance process involves many ongoing, quarterly, and annual activities. Exhibit 18.1 is a very high-level compliance process flow diagram.

During the activity of *establish compliance framework* (see Exhibit 18.1), the first step is for companies to establish the compliance time frame and determine dates and milestones for internal controls to be put in place. Next, companies need to establish a compliance steering committee. This includes establishing a compliance program with documented procedures (including guidelines for the committee to operate within), identifying key compliance personnel, and establishing an internal controls framework. Furthermore, program progress needs to be reported to the board of directors periodically. Both program establishment and progress reporting involve decision making, collaboration, and communications. Content, such as e-mail messages, online collaborations, and meeting minutes, is essential in compliance program establishment and should be managed systematically. ECM can help companies to achieve this by providing security and records management based on the corporate retention policy.

Next, companies need to *assess risks.* In this activity, companies need to analyze current business processes, map processes to financial lines or key accounts, identify risks, estimate risk likelihood and impact (risk exposure), establish the risk library with mitigating controls, and state corporate risk appetite. Risk assessment and control identification involve many constituents, such as business

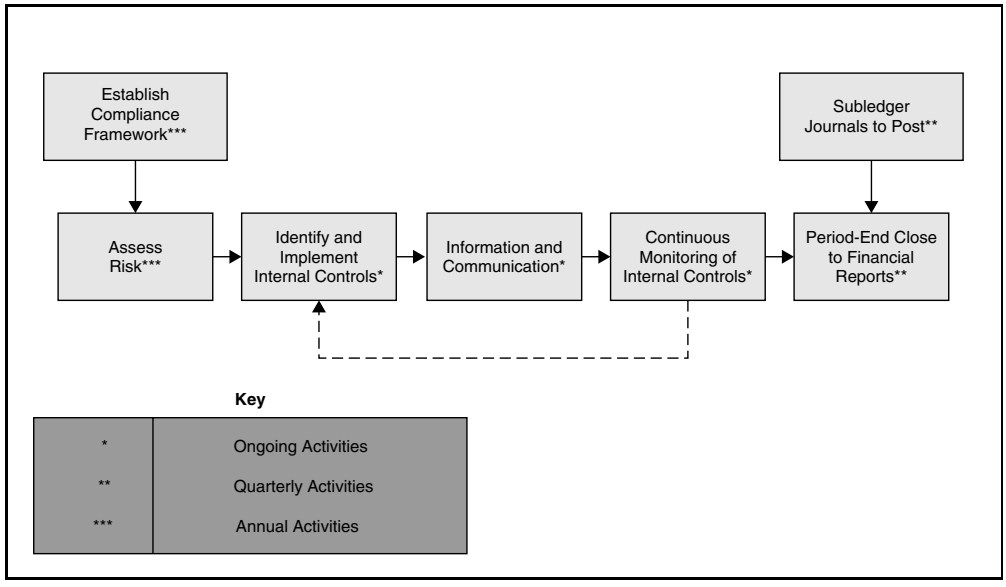


EXHIBIT 18.1 HIGH-LEVEL COMPLIANCE PROCESS

process owners, the information technology (IT) department, internal audit, and executives. Effective communication is essential in ensuring buy-in from different parties. For instance, business process owners are responsible for process documentation; the IT department performs actual process orchestrations; controls identification for risk mitigation is probably done in collaboration between business process owners and auditors; risk appetite is likely to be determined by executives. A full audit trail of document sharing and change history should be kept according to corporate policy. Change management with approval work flow on shared documents can be provided through ECM. With integration, the risk library can be imported and exported from ECM to compliance applications. ECM can then keep static images of different versions of the risk library from compliance applications, making electronic discovery (e-discovery) easier in time.

Identify and implement internal controls is the next step in the compliance process. Companies need to define and design test procedures for control evaluations, steps in carrying out these procedures, and any related work papers to be used in control testing. Companies then perform initial testing to determine both design and operational effectiveness. With these results, further fine-tuning and new controls might be needed to establish a reliable control environment. With this initial testing, *information and communication* should be carried out to the audit committee. Documentation of results, opinion evidence, and key metrics for evaluating internal controls should all be communicated clearly. After the initial testing, *continuous monitoring of internal controls* should be performed periodically through self-assessment and auditing. During auditing and testing, evidence such as work papers, samplings, and assessment questionnaire results are all critical in supporting opinions. This content should be stored in ECM and linked to related control testing results.

Last, companies need to file financial statements with the government. This is represented in the high-level compliance process as *period-end close to financial reports*. Financial close and reporting could be an automated or a manual process. The products of this process are financial statements. When companies assert to their control environment, financial statements of that period are important support documents. Any material change should also be documented and reported with the assertion filing. These sensitive contents should be stored in ECM's highly controlled folders as defined by retention rules and through individual folder properties.

18.3 STANDARD REQUIREMENTS

Enterprise content management (ECM) can help companies to manage content with security, streamline business processes, and decrease risk associated with inappropriate document destruction and proliferation. Niche vendors have limited functionalities that are offered at a lower cost; large vendors have deeper functionalities that are more expensive and more complex to implement. Regardless

of which vendor the solution is from, the following is the list of standard requirements that any ECM vendor should provide:

- *Library services.* To ensure integrity of contents stored in ECM systems, the basic library services should be available. These functionalities include version control, check in/out, and document-level security.
- *Repository search.* To fulfill legal discovery needs, ECM should provide both metadata and full-text-level search capability. If a company is asked to provide all supplier contracts above $2 million for the past five years, the company should be able to do a simple search on all supplier contracts and gather all necessary information quickly and accurately.
- *Document routing.* Documents approval should be routed to the different constituents based on predefined work flow. ECM systems should have a set of out-of-the-box routing flows that allows for modification. The system should also allow users to perform ad hoc routing.
- *Central user administration.* Corporate policy dictates user access for folders on the ECM system. A centralized user administration can help to enforce corporate policy. This way, only a few administrators can provide access to users on different folders. It is easier to control access and its changes with a centralized ECM access management.
- *Support for all popular text file formats.* Since content could be any format (e-mail, image, documents, chat message archive, etc.), ECM systems should be able to handle all of them, providing library services, search, routing, and security capabilities.
- *Document imaging.* Besides digital documents, there are also physical documents that companies need to manage, especially if the company is still running on paper-based processes. This kind of static document should be managed according to corporate policy also. ECM that supports imaging can help in achieving security and compliance for physical documents through scanning.

18.4 ADVANCED REQUIREMENTS

On top of the standard requirements, ECM systems should have optional add-on features for more complex requirements:

- *Document-centric collaboration.* Communication is important in compliance, whether it is among audit committee members or between operational managers and executives. During the decision-making and reporting process, there are documents to be shared, changes to be made, and approvals to be acquired. A document-centric collaboration feature from ECM systems can help facilitate this process and ensure all decisions and changes are kept in the full audit trail.

- *Compound documents support.* In financial statements filing, there are final reports that can be a consolidation result of other documents. The ECM system should allow rules and formats to be set up to generate the final documents automatically, once the approved and locked-down source documents are available on the system. For example, the 10-Q is a quarterly report that includes critical documents of the period, such as financial statements, management discussion and analysis of financial condition and results of operations, market risk disclosures, and controls and procedures. Once the financial statements are finalized and other critical information is properly documented and stored in the ECM system, the final 10-Q could be generated automatically for executives to review and sign off on.
- *Digital assets management (DAM).* DAM is a form of ECM, but for digital assets specifically. It provides security, library services, routing, and retention capabilities for any form of content in a binary source with the right-to-use, such as textual contents, images, and multimedia files. Companies need to file 10-K reports with the Securities and Exchange Commission (SEC) annually, and the relevant financial statements and proxy documents could be stored as static locked-down image files for record keeping or compound document generation. With this functionality, companies will be able to treat digital assets with special rules and work flow through ECM systems.
- *Records management.* The international standard on records management, ISO 15489:2001, defines records management as "The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records." A record could be in any form of tangible or digital format, including both structured and unstructured data. It is essential, with respect to compliance, for corporations to have records retention policies. Records management can store and enforce these policies automatically through predefined work flows. Records retention determines the content life cycle, including destruction and archiving time line and format.
- *Rule-driven work flow.* Work-flow support is a standard functionality for ECM systems; a more advanced requirement is to have rule-based work flow. Companies can define rules using a rule engine, and the ECM system will route tasks through a work flow based not only on sequential definition, but also on triggers, such as those from threshold settings. For example, process documentation change should be routed to process owners for approval; if the changed process is mapped to a financial account that is above $3 million, the process documentation change approval should be routed to the vice president of finance as well. Decision points such as

these in routing are essential in providing flexibility for companies with complex operational needs.

- *Web content management (WCM).* WCM refers to the discipline and technologies of publishing and managing content via the Internet, intranet, and extranet. It enables organizations to create and manage content through the Web. WCM should effectively manage increasing volumes of content and enable business users to author content and participate in the Web content management process within the boundaries of corporate policies.
- *Process management.* With the support of process orchestration, ECM enables business users to create, modify, and retire processes that are related to content management with a graphical user interface (GUI). This empowers business users to create process flows that are needed, reduces the learning curve for new users, and eliminates the potential discrepancy between what business users want and what IT administrators set up in the work flow.
- *Windows Explorer.* Business users are very used to Microsoft products. The usual way to find and locate documents on any desktop/laptop computer is through Windows Explorer. It can significantly increase productivity for business users if the ECM is integrated with Windows Explorer, so that users can search, locate, and open files located on the ECM server as if they are on the desktop. Needless to say, security should be enforced for accessing files on ECM systems from Windows Explorer.
- *Advanced security.* On top of basic security requirements (access management of users to folders), ECM should also provide optional advanced security features. These include fine-grained permission at the folder and document level, access management in groups or users, and predefined but changeable roles for document access.

18.5 NEXT GENERATION ECM SYSTEMS

Besides some new requirements, next generation ECM systems mimic many advanced features described earlier. The difference is that next generation ECM systems should be on an open standard architecture. This implies that all features should be extensible to multiple content management systems. For example, retention policies can be enforced across multiple content management systems within the enterprise. The following focuses on new requirements:

- *Web services technology.* In order to ensure enterprise-wide access and utilization of the ECM system, it is essential for the ECM system to be on an open standard architecture. Web services technology allows different technology platforms to communicate among themselves through standardized services. This enables business users to access data on ECM

from any other application without compromising security. For instance, a new business user from the order management system can access process documentation (stored on ECM) to learn how to place an order, so that he/she can follow the defined order entry process.

- *Federated search.* Federated search means accessing data from disparate databases with queries in appropriate syntax, merging the results, and presenting these results in a unified format allowing multidimensional views. This requirement applies to both structured and unstructured data. Hence, for unstructured data (content) to be searchable enterprise-wide, ECM systems need to support federated search. It means that even if the company has a local document management system in China (apart from the main corporate ECM system), the search result can be comprehensive. Therefore, enterprise-wide information can be considered as being stored in one central repository, even if it is not.
- *Compliance solutions integration.* Content management is essential in the compliance process, which is handled in another system. Ideally, the ECM system should have integration with the compliance solution to report on policy changes, documentation modifications, and enforcement of security policies in different folders. This improves productivity of compliance processes and provides testing results, such as those for retention policy enforcement and document change management, automatically.

18.6 CONCLUSION

There are many documents involved in the compliance process, such as process documentation, audit committee meeting minutes, and audit opinion evidence. ECM systems can help to manage this sensitive content according to corporate policies with security while keeping a full audit trail along the way. These translate into productivity improvements in content management and higher reliability of the compliance environment, because ECM systems themselves are automated controls. Next generation ECM systems can help companies grow into the vision of having a single source of both structured and unstructured data for enterprise-wide federated search or provide the same convenience even if that is not the actual situation. Critical compliance needs, such as collecting data and e-discovery, will be made less costly, easier, and more reliable through ECM systems.

For purchasing considerations, price is one factor, but not the only one. Companies should investigate their current and future functional needs for content management. Making sure that the current investment is able to grow with requirement expansion and user and content volume increase is essential in investment decisions. Other considerations include usability, vendor viability, and architectural flexibility.

References

Shegda, Karen M. 2006. Document Management Questions from the Gartner Midsize Enterprise Summit (June).

Shegda, Karen M., and Kenneth Chin. 2005. Document Management Choices Improve for SMB Audience (April).

CHAPTER 19

ENTERPRISE SEARCH AND AUTOMATED TESTING

Scott McElhaney
Saker Ghani

19.1 CURRENT STATE OVERVIEW

(a) INTRODUCTION. Enterprise search—is it the newest killer application for compliance in the enterprise? Maybe so, and one would certainly draw that conclusion when speaking with any number of the enterprise search companies in the market. Much of the technology around enterprise search that exists today is touted to come with do-all, be-all capabilities—a modern-day panacea to an age-old information access and retrieval problem. Upon closer examination, though, one will not fail to notice that a number of caveats plague most solutions, foremost among them being that it is imperative to build "your" own technology around "theirs" in order to meet the data and information goals for compliance requirements, content management, or any other segment whereby search may be a useful component of your enterprise information technology (IT).

If you ask the folks at Google, Microsoft, even Oracle and other enterprise search companies about compliance and regulatory solutions, their response is

somewhat similar: End-to-end compliance is too large and too complex a concept for any one company to tackle, and enterprise search is a small but potentially significant component of an arsenal of tools and technologies available to help enterprises meet their compliance requirements. Many larger companies have partnered with other technology and consulting suppliers to fill the remaining gaps.

The largest of the search-only companies, Google, states that it is primarily and fundamentally a search technology company, with the vast majority of its R&D dollars being spent on the development of search itself, and not the peripheral issues surrounding the effective leveraging of search to solve complex business problems. Many of these search-only companies, Google included, rely on partners to extend the reach of search into other areas such as security and compliance. Search companies and suppliers that are in the compliance business focus on niche areas, including storage, document retrieval, or e-mail search, for instance. At the time of this writing, we are unaware of any company that is considering an end-to-end search solution for enterprise compliance.

At a high level, most search companies sport very similar technologies and typical processes: begin by locating the data (also known as "crawling"), then store the located data for later access, and finally present (known as "serving") the data to the user. One of the major differences among the search technologies of these companies is the distinct mechanisms through which the information is crawled and through which it is served. A number of solutions focus on searching intranets (static sites or portal-driven sites), while another group focuses on content repositories (content management) and enterprise applications, while yet another group focuses on both through adapters and plug-ins.

The big secret and primary differentiator for these companies—often the single most important deciding factor affirming the search solution's claim of providing increased customer value—is the algorithm used to build the intelligence around what the user sees as a result of the search. In fact, search relevance is among the central intellectual properties by which search suppliers are typically evaluated. Speed is another. And herein lies a central challenge to the relevance dilemma—namely, should relevance be particular to or agnostic of the domain under which a search query operates (compliance in this case)? In other words, should a search solution supplier provide regulation specific relevance, or should the relevancy model be void of particulars and focus instead on a wider set of heuristics and algorithms to find relevant matches?

Of the numerous systems available in the marketplace, some sell themselves as being open, full of functionality and scale and with an enterprise focus, while others build their enterprises solutions based on successful products in the consumer Internet search space. Google, foremost among the latter types and the self-accredited master of search, has adopted a general search algorithm, the now-famous PageRank, to grade relevancy. It is still too early to tell whether an agnostic or particular relevance model will stand the test of time. Both trains of thought have produced anecdotal but powerful evidence to support

the superiority of their particular methods. However, while there are important differences between Internet and enterprise search requirements, the success of Internet search engines' ability to locate highly relevant content ensures that the agnostic relevance model will always remain a viable contender in also powering the enterprise search solution of choice.

We have studied and personally reviewed more than a handful of these systems, and in the end our conclusion is that it boils down to marketing power of the supplier and the opinion of the buyer.

Search as an enterprise technology is still in its infancy. Enterprise search for compliance and automated testing has been only superficially dealt with by the mainstream. The market opportunity for search in simplifying rigorous processes and manual activities within enterprise compliance is large, new, and ripe for the taking.

(b) DEFINING ENTERPRISE SEARCH AND AUTOMATED TESTING. Defining enterprise search and automated testing is easy. What is difficult, rather, is defining compliance and also where search should fit in the larger compliance-based enterprise IT architecture. Each enterprise has its own set of compliance requirements, among them Basel II in banking, Solvency II in insurance, and such corporate governance regulations as Sarbanes-Oxley (SOX), new e-discovery rules from the U.S. Supreme Court, and so on. But as each enterprise has numerous groups working toward these ends, and as these groups often manage their efforts in radically different ways, it becomes increasingly difficult to create an IT environment to which an enterprise search solution is well suited. As always, it is best to start with a small pilot with the eventual goal of moving toward the golden ring.

In general, a high-level definition of enterprise search and automated testing strategy should consider the following tasks:

- Identify what data will be exposed to the search function.
- Identify how the required data from across all relevant systems will be indexed.
- Provide the required security access model for the data.
- Provide the capability to dynamically correlate the data.
- Provide auditors, internal IT, executives, and internal business with the ability to use automation for both auditing and ongoing operations.

(c) LOOKING TOWARD AUTOMATION. Many companies are looking to automate testing and other areas within the enterprise, and many suppliers have responded to this need by developing and providing niche solutions to assist with this. Organizations tend to rely on suppliers not only for the strategy on how best to automate certain functions but to identify areas and opportunities to help improve their own internal compliance programs. Relying on suppliers is

fine as long as the advice provided is put into perspective, that perspective being that the typical supplier will generally help solve just one aspect of the overall compliance program. After all, most advice coming from suppliers, while with the best of intentions, is usually self-promoting and designed primarily to sell more licenses, hardware, and services.

Looking toward automation requires an organization to take a step back and acknowledge that while enabling automated testing might be an auditor's dream come true, using enterprise search to do so while relying on individual tools provided by distinct suppliers will make the realization of this dream very challenging. Enterprise search suppliers have begun to build in capabilities that can be fully utilized for automated testing. Having said that, it is imperative to remember that such capabilities have yet to be integrated specifically for automated testing or compliance purposes. In the section "Types of Enterprise Search Tools" we will demonstrate how these capabilities can be customized toward fulfilling automation and compliance requirements.

(d) ENTERPRISE SEARCH CONSIDERATION CHECKLIST. As previously mentioned, enterprise search for compliance is still in its infancy. In fact, enterprise search itself as a true business solution is relatively new. The precursor to any successful enterprise search implementation is a well planned and thought out global strategy around information access, retrieval, discovery, and search. Being able to answer questions about why search is vital for one's organization, what problems it will solve, and what functions it will enable, and having a general sense of the cost-to-benefit ratio and also the cost of not doing it is a must, even if done so at a somewhat high level.

Before any move toward implementation, it is imperative for the enterprise's business leadership to develop a well-thought-out understanding of the organization's search needs, including a rationalized value of an organization-wide search initiative. Any implementation coming at the heels of a powerful search strategy will allow one to make correct decisions about the organization's long-term search and data retrieval needs, and will ease the adoption of search technology to solve those myriad needs. Of course, in a true strategy session there will be many more valid questions raised and answered, but beginning with these is a great start.

The following is a list of things to consider before delving into an enterprise search implementation:

- Know what type of data you have. Most data is accessible by current search technologies but some typically require more work to get to.
- Know where your data resides. Inaccessibility is not a deal breaker but is much easier to deal with when most, if not all, of your data repositories are thought of up front.
- Understand the security requirements, and know the difference between authentication and authorization. Authentication is the access permission

to connect to a data store, while authorization is the permission providing access to the individual documents or data itself. It is one thing to grant the right to search, but it is an entirely different thing to grant permission with regard to documents that are accessible to some and restricted to others. Who has access to search results is, after all, *the* crucial detail.

(e) TYPES OF ENTERPRISE SEARCH TOOLS. In working for one of the world's largest management consulting and system integration firms, the present authors have seen many enterprise search technologies that span the entire gamut of solution sizes, from the largest to the smallest. Having worked closely with Google, Microsoft, and numerous other search suppliers, we have had the opportunity to examine most, if not all, major enterprise search solutions available as of 2006.

And what we've found is that while there are literally hundreds of tools for search in the marketplace, most of them are associated with a particular hardware or software solution, or provide a niche search functionality (e.g., searching network storage devices, e-mails archive repositories, or for legal discovery). Despite the functional focus, most suppliers work on the premise that *their* technology is solving the world's information access problems, or at least has the potential to with the proper amount of customization. Reality, however, paints a different story. No one supplier has solved the numerous challenges intrinsic to a search solution, albeit some have made significant progress in their particular search domains. We make this conclusion after having witnessed the outcome of numerous enterprise search pilots conducted at major corporations around the globe. The same consistent theme rang true then as it does now: Enterprise search has huge potential in an organization, but the overall technology is still in its early stages of evolution.

This rings especially true for utilizing search for compliance. Most enterprise search implementations are focused on finding particular documents inside an organization, similar to what one finds during a typical Internet search of web sites. Another use for search within organizations gives external customers better product searches for business-to-customer (B2C) marketplaces. For compliance-related solutions, one would have to consider a multitude of search products/suppliers to collectively provide an end-to-end compliance solution. Again, most successful enterprise search products are successful insofar as a narrow search domain is concerned, and one can easily detect an inverse relationship between an enterprise search product's perceived success and the breadth of the search domain it operates under.

Security controls around the exposure of highly sensitive data have not been properly solved by any of the suppliers at this time, and even less so as a standards-based uniform model adopted by a large number of suppliers. As most search solutions are designed to integrate with existing systems, ensuring the continued soundness of the target system's security model can be tricky and is often inadequate. One such example is single sign-on (SSO), where the absence

of widely adopted industry standards makes standardization difficult for a supplier to support. In fact, it takes an enormous amount of customization to get around the security challenges inherent within an SSO implementation.

From a search supplier's point of view, of course, this makes sense. As stated by Google when asked why it does not provide a fully robust security model around its search appliance, the response is a valid one: Google is a search technology company that specializes in meeting the most important needs of search itself, namely speed and relevance. Google does and will include a security model built into the product, but it cannot, and was never meant to, completely meet all security requirements for all organizations. Rather, Google relies on its partners to develop and share best practices around security for their products.

Emerging security standards, such as Security Assertion Markup Language (SAML), will likely bring some much-sought-after relief to the typical challenges of integrating a search solution around systems with much-nuanced security needs. Until then, and resulting from the inherent security concerns, many search projects will likely continue to be put on hold or piloted until either the supplier or the organization can meet these requirements.

(f) IMPLEMENTING AN ENTERPRISE SEARCH TOOL. Implementing enterprise search tools has so far been an exercise in cloning or closely cloning google.com, yahoo.com, or other Internet-based search web sites. Mostly used for searching nonsecure content, the typical solution will gain superuser access to all public documents, feed them into some search repository where they will be indexed for speedy retrieval, and then be served by the tool itself in response to a search query issued by some authorized user. Typically, the solutions allow administrators to fashion the search results in such a way as to contain the necessary user interface (UI) and branding considerations one would typically find on a corporate intranet. This effectively shields the user from discovering the fact that the just-conducted search was powered by an external system.

Partners of search suppliers have gone as far as to build their own framework around the technology for two major reasons, the first of which is to fill the gaps in security, supported data types, and any other functionality not inherently supported by a particular search solution. The second reason is to be able to abstract away the solution itself, giving partners the ability to deploy any number of different search solutions, each with a specific design and search need. We alluded to this earlier when providing the example of searching network storage and e-mail archives. By building an external framework around the search component, partners and suppliers can readily be assured of not being too committed to any one search product and supplier.

As an example of these difficult security issues, consider the situation of a present client of ours, a large aircraft manufacturer. Having heavily invested in a search technology it purchased and deployed for thousands of its North American

employees, it is now greatly concerned by the security limitations of search solution, discovering two years too late that the stringent security needs of the organization cannot be met by the primitive security capabilities of the solution.

For over two years the corporation has been providing limited search capabilities for mostly public documents on the intranet. To maximize the return on investment (ROI) made in enterprise search, the client wanted to enable its employees to search for secure content also. They quickly discovered, however, that although the search product claimed to support single sign-on (SSO), a technology this company had already standardized on, the search product could not be integrated to meet the organization's security policy requirements. In reality, the product did support single sign-on, but as there is no widely adopted industry standard around SSO solutions, the mechanism through which the search solution solved SSO was incompatible with the needs of the enterprise.

The workaround to solve the security issue on their own was too complicated and costly. At this point the client has gone back to the drawing board to reevaluate the technology and has opted, instead, to partner with a third party that had already anticipated these problems and had built frameworks to support our client's particular security needs. At the time of this writing, this client is considering a pilot project to offer users the ability to search for secure content using a third-party framework integrated with the search solution itself.

Implementing search for compliance is complicated because it requires access to both nonsecure and secure data behind the firewall. Planning the solution is the key to success or failure, as with any enterprise project regardless of project type. Security, security, and security are the number one, two, and three issues with implementing search not only for compliance but in general within the enterprise.

If you are looking for compliance around segregation of duties (SOD) in an enterprise resource planning (ERP), e-mail, desktops, document storage, or any other niche area, there are hundreds of suppliers ready to solve your issue. But if you are looking for true enterprise search for global compliance, be ready for a minimum commitment of one year. Solving your security issues will be the number one program risk and will most likely consume most of the project cycles. Make sure to have representation from all levels and business units. It will be necessary to explain the security risks around data exposure and also the level and type of impact such exposure will have on the organization.

19.2 CHALLENGES IN APPLYING BEST PRACTICES

Given the relative novelty of most solutions, the industry has not been able to agree on what constitutes best practices for enterprise search and compliance. To date each supplier has its own set of standards built around its technological capabilities and vision. Having spoken with countless suppliers and analysts over the years, we have discovered that there is really no observable collective effort to create industry-wide best practices. In a typical compliance project setting, search

follows the target compliance model being worked toward, and you would ensure, for example, that the search implementation is internally certified against your Basel or SOX frameworks where applicable.

Considering the fact that two of the top three search companies have vehement disregard for each other's solutions and technologies, it is hardly surprising that there is no agreed-upon best practice, and the future will likely produce multiple sets of better practices. Much will depend on who ends up supplying the tools, technologies, and services for your enterprise. In the end your number one problem will still be meeting security needs around data.

19.3 CASE STUDY: GLOBAL OIL AND GAS EXPLORATION CORPORATION

(a) CHALLENGE. One of the world's largest oil and gas exploration companies based out of the Midwestern United States needed help getting a handle on how to document, store, and retrieve compliance processes and procedures mainly for SOX related issues utilizing enterprise search technologies. The program was separated into four distinct phases over a 16-week period.

(b) PHASE 1: ENTERPRISE SEARCH STRATEGY. The program began by establishing the governance and management structure for the program itself. Business and IT executives met for a series of strategy workshops focused on determining how search could be used to reach the end goal, including ongoing compliance and automation where applicable. As has been alluded to previously, careful initial planning is perhaps the single most important aspect of any enterprise search adoption project.

During this stage, the group spent a significant amount of time focusing on business considerations and requirements around search: What business problem will it solve? What function(s) will it enable? What is the cost of not doing search? And what is the overall value of search to this particular organization? Technical requirements were gathered next, and the team spent a great deal of time answering the following questions: How big is our information access problem, and how can we quantify it? What is the scope of the search reach? What information systems need to be targeted? How do we preserve data security so that both authentication and authorization concerns can be effectively addressed? This phase concluded by drafting the program's work plan, establishing an enterprise project management office (PMO), and developing plans for change management.

(c) PHASE 2: SOLUTION VALIDATION. To validate the solution, the company's leadership had to undertake a number of technical exercises, which included the refinement and augmentation of specific functional requirements of the solution, designing of future processes, development of user interface specifications, development of an analysis matrix to help identify the target information systems and categories, and finally a well-laid-out data strategy and deployment plan definition.

Another crucial technology challenge that was dealt with at this time was defining the access requirements and capabilities to ensure that the search technology had adequate access to all the information it needed to search upon. Some of this was relatively straightforward, with the search tool itself providing a number of mechanisms to ensure easy access and integration. A number of systems, however, could not be directly supported by the solution, and this phase invested a good deal of time and effort to define the data extraction processes to enable the search tool's reach. In other words, most search tools, when incapable of directly integrating with an external information source, will typically provide a mechanism for those sources to be fed into the search tool itself, thereby facilitating a wide range of potential data sources to be searchable through enterprise search.

Ultimately, more than 70 percent of the company's requirements were met through the standard functionality of the solution. To get to 100 percent, a series of custom applications and interfaces had to be developed throughout the program's life cycle.

(d) PHASE 3: SOLUTION DESIGN AND BUILD. The actual hands-on work was completed during this phase, with the custom application and interfaces development effort going through the typical development life cycle. The program team worked with company leadership to elicit feedback and start the process for solution training. Testing was executed during this phase, as was the development of data conversion tools and processes and interfaces. A major usability component during this phase was integrating the new enterprise search functionality within the plethora of existing information portals. For example, the company intranet, which already had a "search bar," was augmented to now provide end users with a list of target sources to search against, thereby unifying the enterprise search function within the portal itself. Many of these access points, peppered throughout the application portfolio, were augmented to enable the newly tooled search technology.

(e) PHASE 4: DEPLOYMENT. Finally, during the deployment stage the program team worked with business units and IT to refine the solution and to make modifications where applicable. Final UI changes as well as close collaboration with the firm's marketing support team produced online training programs, user's guide material, as well as user interface adjustments for branding and other considerations. This phase also saw the final completion of all technical and functional testing. Once testing was complete, the solution was taken live across the organization in a pilot.

In just 16 weeks, the program quickly and successfully implemented a pilot search solution that included an appliance from a major search vendor, multiple custom connectors for disparate sources of data, and defined processes for ongoing operations.

An example of an automated process was to provide for automated three-way matching used by internal as well as external stakeholders. Providing

for automated three-way matching saved the company not only thousands of dollars but also a foundation for future solution enhancements. At first, this automation capability was thought to be of little value and too confusing for the business units prior to its deployment. By deploying it in a pilot, this was used as a springboard for buy-in for future versions.

References

Section 331 of Title 28, United States Code dated April 12, 2006.

CHAPTER 20

WHAT TO LOOK FOR IN AUDIT OPERATIONS APPLICATIONS

Julia Koo

The highest priority of any company's executive is to increase shareholder value. Moreover, Sarbanes-Oxley (SOX) has put something further on executives' minds: criminal liability. This chapter tells how an audit operations application addresses both of these issues. Furthermore, it discusses what considerations there are for choosing the one application that suits your needs—for both today and tomorrow; it analyzes today's pain points, presents current basic and advanced feature requirements for these audit operations applications, and foresees next generation applications' architecture.

20.1 AUDIT PROCESS

Audit is not a new concept to companies. The internal audit department's and external auditors' involvement in ensuring financial reporting accuracy has always been a part of doing business. Exhibit 20.1 shows an example of a simple internal audit process. Companies may have different versions of this process.

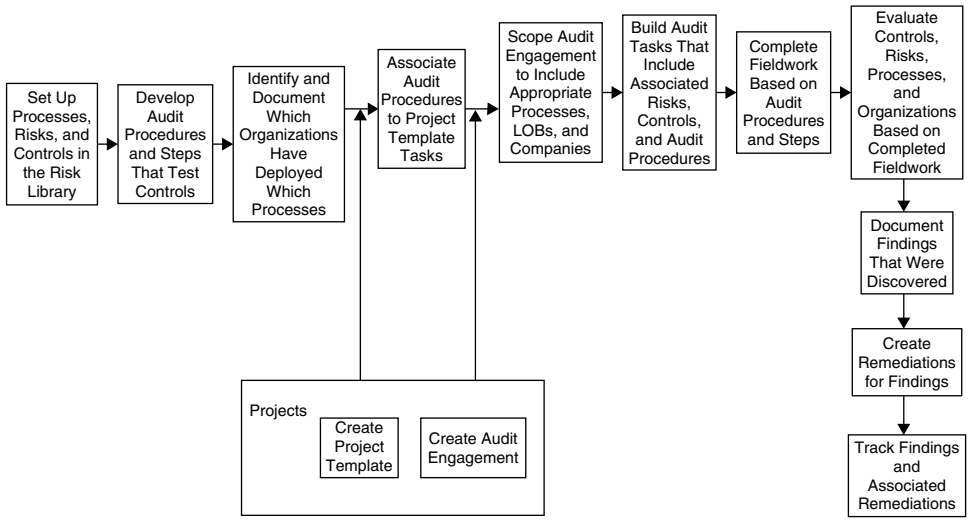


EXHIBIT 20.1 INTERNAL AUDIT PROCESS

Starting from the basic setup in *risk library* as a centralized repository to allow data reuse, companies need to work with different constituents from different lines of business to draft and finalize business processes definitions, risks associated with each process and subprocess, and controls established to mitigate these risks. These processes, risks, and controls usually have a many-to-many relationship; hence any changes made to these objects and relationships should be tracked and should allow all involved parties to see the changes made and approve accordingly. After controls are identified and put in place to mitigate risks, companies need to ensure periodically these controls are working properly. This is usually done by the independent internal audit department to ensure neutrality. In order for internal auditors to carry out tests, audit procedures and testing steps have to be predefined collaboratively between business process owners and internal audit.

For companies with multiple organizations, especially internationally corporations, processes could vary in definition from one organization to another. This could be due to different national laws or adaptation to local business practices. Regardless of these factors, companies need to instantiate processes in organizations and make definition changes accordingly to reflect the true nature of each organization's operational process. Some organizations don't even deploy all processes. Therefore, instantiation of processes at organization level is essential in representing operations correctly for audit purposes.

To ensure controls effectiveness, companies need to do periodic testing and auditing. The general practice is to have the audit project set up and scoped to

perform testing on certain areas, such as in a particular organization, for a certain business process, or for any particular regulation. Because these audit projects could be performed periodically, it is a general practice for companies to have created audit project templates that include all the necessary work papers. So when a project is needed, all the auditors need to do is to pull out the template and create a new project based on the template. The template could include the scope of testing, tasks to be performed, predefined spreadsheets as work papers, and any supporting documents.

At the testing time, auditors perform the testing steps and record their evaluation opinions. These opinions need to have bases, so storing supporting evidence and linking them correctly to each opinion is essential for future reference. During testing, auditors are likely to discover trouble areas and places that need to be improved. These concerns should then be documented, assigned, and tracked. A full audit trail is needed to prove that weaknesses, especially material ones, have been discovered, investigated, and mitigated. For this purpose, companies usually use findings or issues to document problems exposed during auditing.

Throughout the audit process, the audit department might have recommendations for improving said process. These improvements can then be proposed to the audit executives, CFO, audit committee, and other constituents for approval. This is a feedback loop into the audit process to improve its efficiency and reliability.

20.2 AUDIT OPERATIONS MATURITY MODEL

A maturity model is usually used by companies to analyze process efficiency. Different versions of this maturity model could be used to analyze the effectiveness of an audit process. The movement from the bottom left corner to the top right corner in Exhibit 20.2 indicates improvement in efficiency of the measured process. The following is one of the possible illustrations of how a maturity model could be used to analyze the audit operations process.

There are five levels in a standard maturity model: *Initial*, *Repeatable*, *Defined*, *Managed*, and *Optimizing*. Level 1 is the initial level where companies are using manual processes to manage disparate information around auditing. Printouts of spreadsheets and documents have to be stored securely in a filing cabinet under a certain order for recovery purposes. For the scope of this discussion, level 2 (*Repeatable*) and level 3 (*Defined*) have been consolidated into one level. At level 2, the process should have been documented but not standardized throughout the enterprise, whereas at level 3, the process has been documented and standardized. For compliance purpose, companies usually achieve level 2 and level 3 together. While they are documenting their processes thoroughly, they also try to standardize them across the enterprise and document any variations that might have been encountered at certain organizations. Hence, level 2 and level 3 are condensed into one level: *Defined*. At this level, audit operations application,

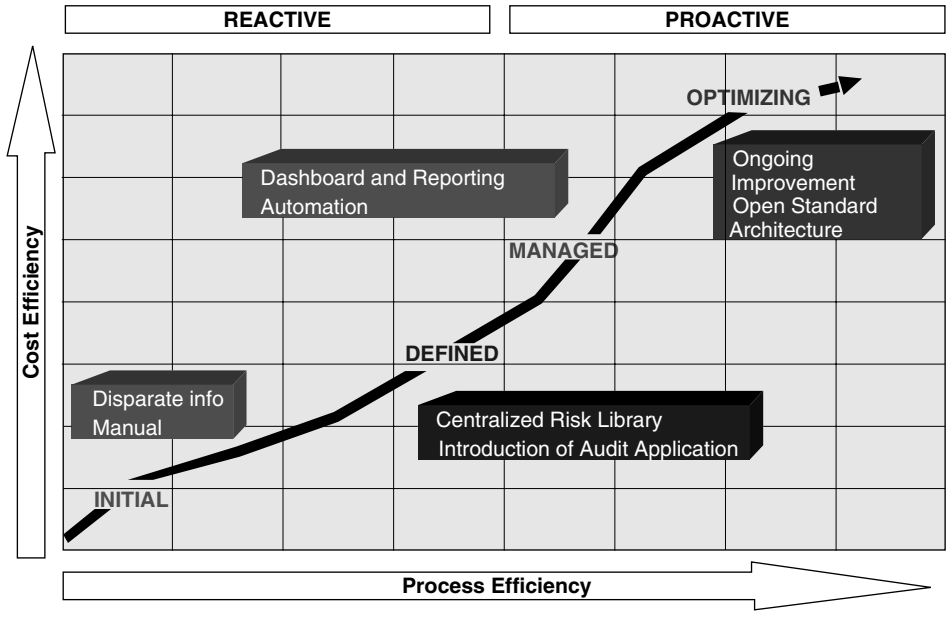


EXHIBIT 20.2 INTERNAL AUDIT OPERATIONS MATURITY MODEL

along with its infrastructure, needs to be introduced to have a centralized repository of processes, risks, and controls and associations among them. At level 4 (*Managed*), performance measures are put in place to measure success. Control automation is also introduced on this level to help in improving testing efficiency and reliability. The final level is the *Optimizing* level. At this level, the audit process is being watched constantly for continuous improvement. It is being tied to the broader corporate performance management, integrated into daily business operations, and infused as part of the open standardized IT infrastructure.

In the following section, this maturity model will be used to analyze the audit operations process in greater detail. It will be shown what companies need from different applications at each level, and what to expect in the future if a movement from one level to another is desired. However, since companies could be very different in nature (e.g., industry, geographical area, budget allocation, etc.), it is up to each individual company to estimate which level it currently is at and which level it would like to be at in the future; then it can plan its budget, resource allocation, and application purchases accordingly.

20.3 BUSINESS PAIN POINTS (LEVEL 1: INITIAL)

Most, if not all, accelerated filers of the Sarbanes-Oxley Act (SOX) have moved away from this level because the law requires them to document their processes, put controls in place to mitigate risks, track findings and issues, and report on

issues and bad business conducts that might have surfaced. It is hard for companies to remain on this level with these SOX requirements. At this level, companies are using manual processes to track audit-related information, including project scoping, testing, evidence tracking, trouble logging, and data reporting. Electronic and physical documents, spreadsheets, and manually consolidated reports are usually the vehicles of the process. Information sharing depends on individuals' gratitude. Reliability of data depends on people's integrity. There is usually a lack of security, access control, and status tracking at this level.

20.4 VALUE PROPOSITION OF AUDIT OPERATIONS APPLICATIONS

There are several reasons why companies should move from the initial level to the other levels:

- Cost reduction
- Reliability enhancement
- Visibility improvement

(a) COST REDUCTION. Audit operations applications should provide a centralized risk library that can be leveraged across all departments and locations. The audit application can also act as the single source of truth of all testing results. This single repository simplifies training for new auditors, increases productivity of existing ones, and allows information sharing with external auditors to become a "click of a button" activity to generate auditor-ready reports on testing results and findings. Furthermore, if a control is information technology (IT) focused or system orientated, testing scripts can be set up in the audit application to generate automated testing results, link those results to a control, state an appropriate control testing opinion, and prompt auditors for opinion review. In addition, this whole process could be repeated at any interval of time at an auditor's preference. This transforms manual testing by auditors into automated control testing by the application. Auditors will only need to review these results. The increased productivity, simplified training, and reduced testing scope for internal auditors will help companies to cut costs.

On top of internal cost saving, external cost saving is also very significant. Companies spent $1 million to $8 million in year 1 of SOX.[1] Most of the expenditures went to external auditors for their time spent in gathering evidence on controls. An audit application allows companies to share internal audit testing results and evidence with external auditors quickly and easily through auditor-ready reports. These reports tend to be in PDF format, which cannot be edited; hence it is trusted by external auditors. With information sharing being simplified, it usually implies smaller test scope by the external auditors before their attestation to control efficiency of the company. With automated controls, the testing time by external auditors will be reduced, even if these controls remain in scope for external auditors. All of this time reduction translates into cost savings for companies.

One advanced feature (a complete features list will be presented later) of audit applications is transaction abnormality alerts. This kind of alert is referred to as proactive controls. It is apparent that if a problem is dealt with earlier, the loss could be managed better and the cost of loss should be lower. Proactive control allows you to do exactly that. Potential problems are sometimes predictable earlier in time through transaction observation. However, manual transaction monitoring or sampling could be costly and error prone. Hence, audit applications provide the capability of rule engines, validation alerts, and trend tracking. With these capabilities, companies can deal with a problem earlier in time, sometimes even before the problem occurs. Change of a policy, investigation of an employee, and discontinuing a supplier contract are all possible resolutions of potential problems, such as fraudulent events and unreliable suppliers.

In short, with audit operations applications, cost reduction can be realized from increased productivity of internal staffs, lower external auditor costs, and transaction abnormality alerts that prompt immediate attention and actions.

(b) RELIABILITY ENHANCEMENT. Automated controls not only reduce costs, but also increase reliability because results come directly from the companies' operational IT system. By eliminating human involvement in control testing, risk of error and fraudulent events can be considered as nonexistent in this type of control.

Audit applications should inherently consist of a work flow engine that mandates the audit process's flow. Areas such as approval and task dependency should be enforced by the work flow engine. For instance, without proper review, high-impact issues cannot be closed. This kind of enforcement can ensure that a standard policy is followed; hence it increases reliability in the data being reported for compliance purposes.

(c) VISIBILITY IMPROVEMENT. With disparate information, reporting is meaningless because data cannot be guaranteed to represent a holistic view of the business. Furthermore, meaningful conclusions can be difficult to reach when using data comparison without a common reference. For example, an issue resolution cycle time in the sales department is 30 days on average, whereas the same measure of the service department is 5 days on average. By looking at this comparison, one might conclude that the sales department needs to improve its issue resolution time. However, a further investigation into the data might be able to paint a more complete picture that the sales department already has good controls in place and all issues are minor ones, whereas the service department is still installing proper controls, so issues are major and have taken a majority of time of managerial resources in that department; hence service performance for the past month had been compromised.

This simple example illustrates how important it is to do analysis in combination with data from different business areas. Reporting solely on audit performance sometimes tells only part of the story. It is essential to have actionable

business intelligence cross different lines of business and platforms that are capable of dimensional analysis. Only with that can executives have true visibility into their business and make accurate decisions. Information is power; partial information is at best incomplete, and at worst it is misleading.

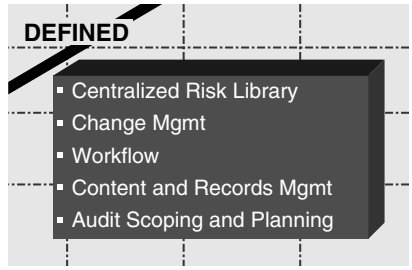
20.5 AUDIT OPERATIONS APPLICATIONS

There are three areas involved in implementing an audit application—namely, the application, content, and implementation. A true end-to-end solution on audit operations should be able to address all three. In other words, the solution should include an application that can be used to address today's pains yet scale to future needs, a set of preseeded content that can be used as a starting point for companies (including a sample risk library and segregation of duties constraints), and a consulting team that can implement the application with optional integration and customization work.

The following section focuses on application requirements for different levels on the maturity curve. Companies should choose an application that can address their pain points today and be scalable to answer tomorrow's needs, especially when the company has a desired higher level in mind.

20.6 STANDARD FUNCTIONALITIES (LEVELS 2 AND 3: DEFINED)

At level 2 (*Defined*), the audit process is defined and documented and all operational processes in the enterprise are standardized. The audit process is repeatable; all processes are documented and can be shared among organizations easily. To achieve this level, the audit operations application should have the following basic standard functionalities:



- *Centralized risk library.* This is a single repository of processes, risks, controls, audit procedures, and testing steps. Both definitions of and relationships among these objects are stored in the risk library. This way, existing object definitions can be utilized for new mappings. For instance, when a new process is added to the enterprise, existing risks, controls, audit procedures, and testing steps can potentially be reused in mapping to this new process.

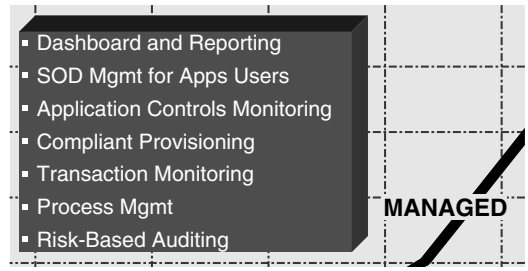
- *Change management.* All objects in the risk library should be under change management. Changes in business are very common. The audit operations application should keep a full audit trail on any changes in the application. The way to ensure that changes are done appropriately is through change management: approval process, versioning, notifications, and change history. This way, changes can be approved, tracked, disseminated, and backtracked.
- *Integration with work flow.* There has to be a work flow or process engine behind the audit operations application. Approval requests, notifications, and alerts can be sent out to appropriate constituents automatically when needed. In addition, a background process definition can mandate the audit process as it is defined in company policy. For example, the company policy could say that whenever there is an audit opinion of "unmitigated" on any risk with high risk exposure (high impact and high likelihood), a finding must be created, assigned, and tracked. The work flow engine can then mandate this policy in the audit operations application by making the auditor fill up a finding template after he/she gives the opinion of "unmitigated" to a risk with high risk exposure.
- *Managing organizations and process structure.* Companies can have very simple or very complex organization hierarchical structures defined in their human resources (HR) systems: lines of business, legal, operational, and so on. There is also the defined master copy of all process hierarchical structures in the risk library. However, when processes are instantiated at different organizations, the structures could have been modified according to local operational needs. All of these predefined structures have to be presented through a simple, easy-to-navigate graphical user interface (GUI). Technologies such as trees can be utilized here. On top of presentations of structures, the audit application should allow end users to create their own organization and process hierarchical structures as part of the personalization feature. Users can then view aggregated data on things like status and progress for their interested areas only. These personalized structures should be created easily with GUIs and drag-and-drop capability and can be shared with other colleagues.
- *Audit projects planning.* Auditing should be done periodically. Sometimes the scope of an audit project is strategic, such as the CFO wants to check control efficiencies in a particular organization because there was a reorganization there last quarter. Other times, the scopes of audit projects are systematic because controls should be tested according to the predefined control testing frequency, controls that are linked to significant accounts should be tested every quarter, or controls that are used to mitigate the risk of company reputation damage should be tested annually. These are all predefined company preferences in testing that mandates scopes of

periodic auditing. The audit operations application should allow scoping, task assignment, and task dependency to be done both manually and automatically through scheduling.

- *Self-assessment support.* Not only auditors test controls, but also business process owners do self-assessments (voluntary control testing) periodically to better understand their processes and improve accordingly. These self-assessments could be done either through surveys and questionnaires or through procedure-based testing like the auditors do. These self-assessment results could help the executives in signing off on their high-level processes and financial statements, along with auditors' testing results. This feature could be seen as a separate application from the audit application because it is utilized by different business users. And companies do keep these activities separated from audit activities. However, the risk library definition could be leveraged here, so that self-assessments that are procedural based could be done without redefining all objects in the risk library.
- *Finding/issue management.* Throughout tests, auditors find trouble areas that should be recorded, assigned, and tracked. Findings and issues are used for this exact purpose. Executives can pay close attention to findings and issues to know what needs to be fixed, who are doing it, and what the progress is in accomplishing it. When findings and issues have due dates, reports like "Past-Due High-Priority Findings" would be good actionable ones for executives.
- *Integration with content management.* All supporting documents of audit operations, such as work papers, process flowchart, and audit opinions evidence, should be stored securely in a content management system. Basic functionalities like version control, security, and check-in/out should be provided to these documents. This integration should be seamless, meaning that shifting between features from audit applications and content management should not be noticeable for users.
- *Data security.* Within an audit operations application, there are many sensitive data. Security is critical in this type of application. Data access management should be done at the most discreet level: role-based security. For example, Peter and Mary can both see the list of control evaluations but, based on their roles in the organization, they will be able to access data differently. If Peter is the owner of the Order to Cash process and Mary is the reviewer on the process, Peter will get to modify data in the audit application, but Mary will only be able to review a view-only version of data in the Order to Cash process.
- *Basic reporting.* Basic online reporting that is downloadable to spreadsheet, PDF, or Word document should be provided for communication purposes.

20.7 ADVANCED FUNCTIONALITIES (LEVEL 4: MANAGED)

At level 4, companies need to have control automation to increase reliability, dashboard, and reporting to measure success and failure. Moving from level 2/3 to level 4 means that companies can realize benefits of cost savings, reliability improvement, and increased visibility by relying more on automated controls, transaction abnormality alerts, and data analysis from different operational areas to resolve problems surfaced in auditing. To achieve this level, the following functionalities are needed in an audit operations application:



- *Audit project management.* More advanced audit project management will improve audit productivity and planning efficiency. Features like milestone tracking, resource management, and Gantt chart presentation should be included here.
- *Automated controls.* This includes three different areas that should be considered, namely segregation of duties (SOD), application controls monitoring, and transaction monitoring.
    - SOD violation means user access to IT systems might have created chances that allow risky events like fraudulent activities to happen. To avoid this, applications should have a set of predefined constraints set up in the system. No new provisioning that violates these constraints can be done without approval. At the same time, existing conflicts in access should be dealt with either by removing certain access or by tracking those users as waived users with documented reasons. Please see the next chapter, "Automation of Segregation of Duties," for detailed discussion on SOD.
    - There are many embedded controls in business applications' setup options. For instance, Match Type is a setup value in Account Payables, and it could be a three-way match or two-way match. Depending on company policy on account payables operation, this implementation option should be set accordingly. Application Controls Monitoring allows the IT department to monitor application setup values such as this, and ensure that patch installation and system migration will not deviate application setup values from company policy.

  - Transaction abnormality reporting can catch risks like fraudulent events in advance or shortly after they occur. Apart from abnormality reporting, pattern watching is another way to catch potential problems using the same idea of transaction monitoring. This requires integration with business applications like the ERP system. A rule engine will sit on top of the transaction system for continuous monitoring on all related transactions. If a rule is broken or a threshold is crossed, an alert will be sent to appropriate personnel for further investigation.

- *Dashboard and reporting.* On top of the basic online reporting from the audit applications, more advanced data analysis and aggregation functionalities should be provided for level 4 applications.
  - Aggregated data is needed for senior managers and executives to view progress and status at a higher level. This requires data roll-up on hierarchical structures, such as the organization or process structure. Dashboards are usually the means of delivery. Graphical representation of data is usually preferred for its clearer and easy-to-digest presentation.
  - Detailed reports are then required to provide next-level details. If the executives need to know more on a particular piece of data, they can drill down to the detailed reports for further analysis. At this level of reporting, data should be presented in both graphical and tabular format.
  - Drilling directly into audit applications for actions to be taken is the next level of convenience that the audit operations dashboard can provide. For example, if the number of open findings with high impact on financials in the European Union is unacceptable, and the problem points to a particular finding in France, found by looking at the detail reports, the executives can drill down directly to the audit application to view details on that finding, make comments, and escalate its status if needed. This drill-to-transaction capability is a more advanced feature of dashboards.
  - Another way to help executives to take actions from dashboards is the integration with e-mail systems and online collaborations. Executives need a way to communicate their concerns or have their questions answered quickly. At the dashboard or detailed report level, executives should have the capability to e-mail, call, or chat with someone right there and then. First, the dashboard allows them to know who that someone is, and second, it lets them communicate with that someone right away through whatever means they want. Last but not least, these communications could be tracked through e-mail, online chat text files, or voice files.
  - Auditor-ready reports are the kind of reports that companies can share with external auditors. These are usually reports in PDF format because they are not editable. On top of that format, these reports should also be

easily personalized for column changes, renamed, hide/unhide columns, graph insert, and so on. Companies need to provide whatever data are required by external auditors and should not provide any more or any less. Personalized reports for external auditors enable companies to do exactly that.

20.8 NEXT GENERATION OFFERINGS (LEVEL 5: OPTIMIZING)

At this level, companies need to think about the future quite extensively and they need to change their ways of seeing audit operations applications. Level 5 means that companies are looking for ways to optimize the audit process continuously. Hence, the applications at this level need to be flexible for changes and very adaptive to new business needs. The new way of seeing applications is to have a foundation that carries basic features and can be easily extended to cover advanced requirements by allowing multiple plug-and-play modules. The enabling technology here is a service-oriented architecture where everything is on open standard that allows data extraction and data exchange among all systems through Web services.

- *Audit foundation using service-oriented architecture (SOA).* The basic and advanced requirements for audit applications still stand. The difference is that, at level 5, everything should be on open standard architecture and enable communications with other systems through Web services.
- *Plug-and-play modules.* Because business needs and regulations change over time, customers cannot buy an application today to cover their needs today and for the future. The solution is to have a flexible foundation and allow plug-and-play modules that can address these future needs, whenever they surface, to be easily installed onto and work with the foundation. The following is a list of modules that customers can even consider today:
  - The next generation audit operations applications should be able to import enterprise resource planning (ERP) and/or business intelligence

(BI) sources of quantitative financial data directly and use them as part of materiality analysis on risks and controls, which is part of audit planning.

- Change of regulations should be imported directly from the publishing web sites into the audit operations application for considerations of risks and controls modification and/or change in audit scope.
- Historically, the database administrators (DBAs) or application administrators have had full access to the database, including the application data and the data dictionary, in order to simplify the application implementation and rollout. A very difficult security problem is then to protect application data, sensitive business information, and privacy data related to partners, customers, and employees from DBAs. SOD at database level will restrict the powerful application administrators from accessing other applications and from performing tasks outside their authorized responsibilities. SOD violation detections at DBA level will then become another critical automated control on the audit operations application.
- Provisioning to system access of new users can be done either manually or with an identity management and access management system. A recent popular requirement is to have compliant provisioning. This means that at the provisioning time, a what-if scenario will be created with the new provisioning content, and if the new scenario violates any SOD constraints, the provisioning will be stopped or flagged as an exception. Appropriate personnel will be notified with this new violation. This implies a communication between the audit operations application that stores the SOD rules and the identity management system that does the provisioning.
- Since Sarbanes-Oxley requires a full audit trail on many things, discussions such as those between executives and audit committees certainly should be tracked. Online collaboration systems allow different parties to share documents, comment, request clarification, respond, and reach conclusions at a secured cyberspace. Information and discussion sequence will be kept in the full audit trail. Minutes of these important meetings can be then generated automatically and be attached to the audit application as an evidence of finding disclosure, for instance.
- Policy management systems store policies for the enterprise, and learning management systems disseminate policies to the enterprise and ensure that all employees have looked at them. Any changes to policies will be made in policy management systems and can be made into an online course that all employees should take if the change is significant enough. Once a course is created, all participants' participation status will be tracked. These policy management and learning management

features, by themselves, could be automated controls that are tracked in the audit applications automatically.

Loss events and whistle-blowers are two ways of surfacing problems from within the enterprise by employees. Should anything become suspicious, a case should be created for the legal department to do further investigation. Investigation management systems track cases throughout their life cycles. In audit applications, issues and findings could be turned into cases. The capability of allowing auditors to create a new case and transfer finding or issue details into this new case should be provided through interoperability services between investigation management systems and the audit operations application.

Standard Functionalities

- ☐ Centralized Risk Library
- ☐ Change Management
- ☐ Integration with Work Flow
- ☐ Managing Organizations and Processes Structure
- ☐ Audit Project Planning
- ☐ Self-Assessments
- ☐ Finding/Issue Management
- ☐ Integration with Content Management
- ☐ Data Security
- ☐ Basic Reporting

Advanced Functionalities

- ☐ Audit Project Management
- ☐ Automated Controls: Segregation of Duties (Preventive and Detective)
- ☐ Automated Controls: Application Controls Monitoring
- ☐ Automated Controls: Transaction Monitoring
- ☐ Advanced Dashboard: Dimensional Data Analysis
- ☐ Advanced Dashboard: Drill to Transaction System
- ☐ Advanced Reporting: Auditor-Ready Reports

Next Generation Offerings

- ☐ Service-Oriented Architecture
- ☐ Audit Operations Foundation
- ☐ Plug and Play Modules: Import of Quantitative Financial Data
- ☐ Plug and Play Modules: Direct Import of Regulations Changes
- ☐ Plug and Play Modules: Segregation of Duties at Database Level
- ☐ Plug and Play Modules: Compliance Provisioning
- ☐ Plug and Play Modules: Online Collaboration
- ☐ Plug and Play Modules: Policy Management
- ☐ Plug and Play Modules: Investigation Management

EXHIBIT 20.3 LAUNDRY LIST OF FUNCTIONALITIES

20.9 CONCLUSION

Audit operations have always been a part of daily operations of businesses. U.S. SOX and related regulations simply put this department under the limelight. The question is now how to make auditing more efficient, cost effective, and reliable, yet flexible enough to adapt to a changing regulatory environment. With changes in regulations and business dynamics, audit operations applications should provide basic functionalities with the extensibility and adaptability to become more comprehensive solutions. Companies can use the maturity model to evaluate their current audit process's level of sophistication. Depending on the conclusion of that evaluation, they should pick an application to address their needs of today. However, if they also have a desired level on the maturity model, their current investment should take that into consideration and they should pick an application that can not only solve today's problems, but also be utilized as a comprehensive solution in the long term. Corporations need to think strategically in their application investments today, in order to be able to utilize their existing investment in the future.

For different levels of the maturity model, there are different requirements for audit operations applications. Some applications in the market today package advanced features as part of the basic offerings as well. Exhibit 20.3 is a laundry list of discussed functionalities that should be included in applications at different levels.

Notes

1. "Study: SOX-Compliant Firms See Drop in Costs in Year 2," by Shamus McGillicuddy, news writer, SearchC10.com, April 21, 2006.

CHAPTER 21

AUTOMATION OF SEGREGATION OF DUTIES

Lindsey Kudo

21.1 INTRODUCTION

Since the Sarbanes-Oxley Act of 2002 (SOX), public companies are now investing time and resources to ensure that effective internal controls are put in place throughout their organization to aid in creating a "new era of corporate accountability and responsibility." While years 1 and 2 of SOX concentrated on documenting key business processes, risks, and controls, the new area of focus by internal and external auditors is segregation of duties (SOD). Segregation of duties is by no means a new concept to the business world; however, the internal controls requirements mandated by Section 404 of SOX have placed a renewed interest in this subject matter. Segregation of duties is a key internal control for any organization to have in place, but also one of the most difficult and resource intensive to achieve.

As companies start to automate their SOX efforts, chief information officers and internal audit departments are evaluating many of these software solutions based on the preventive and detective SOD capabilities. While actual job titles, business processes, and sizes of operations will undeniably vary from organization to organization, large and small organizations worldwide all have an interest in

enforcing SOD rules. Many companies are facing internal and external pressures from the marketplace to evaluate the SOD rules that are in place within their organizations. In large this can be attributed to governing acts such as the United States' SOX, Canada's 52–111, the United Kingdom's Turnbull Guidance and Combined Code, the Organization for Economic Cooperation and Development (OECD) Principles, banking's Basil II, and insurance's Solvency II.

21.2 DEFINING SEGREGATION OF DUTIES

While SOD has become a compliance buzzword, let's take a moment to really define it. SOD should provide the assurance that no one person has the physical and/or system access to control a business process from conception to completion. For example, no one person should have the authority to:

- Initiate a transaction
- Approve a transaction
- Record a transaction
- Reconcile accounts related to the transaction
- Handle related assets

Specific examples that illustrate these concepts are:

- The employee who requisitions the purchase of a good or service should not be the same employee who approves the purchase.
- The employee who has the authority to approve the purchase of a good or service should not be the same employee who reconciles the monthly financial reports.
- The employee who has the authority to approve the purchase of a good or service should not be able to obtain custody of checks.

Segregation of duties is a key component to maintaining a strong internal control environment as it reduces the risks of fraudulent transactions. When duties for a business process or transaction are segregated, it becomes more difficult for fraudulent activity to occur as it would involve collusion among several employees.

21.3 LOOKING TOWARD AUTOMATION

While the first year of SOX compliance was a race to complete process documentation and risk and control matrices, many companies did not actively acknowledge and evaluate segregation of duties within their organizations. Although internal and external auditors may have not reviewed or commented on segregation of duties during the first year of attestation, the majority of them are now taking the time to revise their audit programs to include SOD in their yearly reviews. With many compliance automation products now flooding the market, organizations must take the time to evaluate their business needs and consider what their auditors will be assessing before they make their selections.

Organizations can be exposed to significant risks when conflicts exist with SOD. When evaluating segregation of duties, auditors are looking for SOD violations in which one individual has access to responsibilities that are inherently in conflict with one another, such as purchasing and accounts payable, purchasing and receiving, general ledger and supply management, and so on. The fraudulent activity or financial misstatement that may occur due to the lack of segregation of duties can be caused either by innocent and unintentional errors or by intentional and criminal fraud. However, despite the intention, organizations can be held liable if they have a lack of adequate and auditable process controls.

21.4 AUTOMATING SEGREGATION OF DUTIES

Currently on the market there are a wide variety of automated compliance solutions that address the issue of SOD. Prior to these tools being available, companies typically addressed SOD through a combination of controls:

- Defining transaction authorizations
- Assigning custody of assets
- Granting access to data
- Reviewing/approving authorization forms
- Creating user authorization tables

The tools that are currently on the market aim to duplicate these efforts as well as provide the organization with reporting functionality on SOD violations (i.e., detective controls) as well as put in place preventive controls. Although organizations may put many of the typical controls in place, as enterprise resource planning (ERP) implementations become more widespread and larger in scope, it becomes overwhelming for departments to keep their manual controls around SOD up to date. As organizations grow, resources are added and an employee's job functions change to mirror the ongoing changes within an organization; this causes these manual controls to become quickly outdated. By not automating SOD controls, there is potentially the issue of SOD controls becoming a barrier in serving the customer. As manual authorizations are often time consuming and require another step in any business process, this takes time away from serving the customer. These new automated compliance products aim to provide organizations with timely and efficient internal controls that do not disrupt their normal business process.

21.5 SEGREGATION OF DUTIES CONSIDERATION CHECKLIST

Traditional methods of cleaning up SOD violations within an organization are typically time consuming, resource intensive, and expensive. Therefore, choosing the right SOD tool is important in order to achieve results that are comprehensive and

address the organization's needs without disrupting the normal flow of business. The following is a checklist of items to consider when selecting an automated SOD compliance program.

- ☐ What issues will the auditors look at?
- ☐ Are there currently products that evaluate SOD specifically for the ERP/financial system that your organization uses?
- ☐ Will you need an ERP expert in order to implement the SOD automation application?
- ☐ Does the application have the ability to evaluate SOD violations across a heterogeneous financial system?
- ☐ What are the required resources and knowledge needed to successfully implement the SOD automation tool, and does the organization have them available?
- ☐ At what level are you interested in maintaining SOD within your organization (responsibility, function, form, etc.)?
- ☐ Does the SOD compliance product come with a library of risks and SOD violations?
- ☐ Does the application evaluate SOD violations across financial modules within the organizations?
- ☐ Does the application support evaluating SOD violations for a multiple organization set up in an ERP system?
- ☐ Does the SOD application provide real-time reporting?
- ☐ Does the SOD application have the ability to do simulation violation checks?
- ☐ Does the SOD application provide an easy method to complete cleanup or remediation activities should a violation occur?
- ☐ Does the SOD application allow for multiple users/key stakeholders to use the product collaboratively?
- ☐ Does the SOD application have the ability to automate mitigating controls where SOD conflicts cannot be eliminated?
- ☐ Does the SOD application have the ability to evaluate historical transactions to evaluate whether violations occurred in the past?
- ☐ Is the organization interested in a tool that will provide enterprise-wide control management?
- ☐ Are there any additional system security features that the application provides?
- ☐ Does the software company also provide any other automated compliance products that integrate with the SOD functionality?
- ☐ What type of reporting does the SOD application provide?
- ☐ Are the reports valid to give to the external auditors?

21.6 TYPES OF AUTOMATION TOOLS

A wide variety of tools are currently out in the marketplace that provide a wide variety of functionality with various hooks into their products. Some of these tools are freeware available for download; others are provided by the large ERP companies or by independent companies that are able to sit on top of the ERP structure and assess segregation of duties conflicts for modules that are part of the ERP system. In most SOD tools, segregation of duty definitions can be defined at the function, responsibility, or group level and enforced through real-time monitoring and prevention of inappropriate system access as defined by the organization. The following section outlines some of the key features to look for when evaluating the various software selections on the market.

21.7 SOD VIOLATION REPORTING CAPABILITIES

All of the segregation of duties applications currently on the market are able to evaluate a financial system for SOD violations based on the SOD definitions defined within the application. Typically reports will highlight the two functions or responsibilities that are currently in violation and provide the user name, the responsibilities granted to cause the violation, and when these privileges were granted to that user. The SOD reports filter or narrow down the information to include violations by responsibility, violations by user, and so on. The reports may also come in various formats to review: dashboards, graphs, standard reports, and so on.

21.8 SOD SIMULATION CAPABILITIES

Segregation of duties simulation capabilities is a feature that is relatively new to the market. This capability allows the administrator of the application or a manager to create a simulation, in which they can alter user's responsibilities and run the SOD definitions against those changes to see if it would create any SOD violations. Some applications also allow simulations to beyond the SOD violation results, allowing the user to see the impact that segregation of duties waivers, the cleaning up of system responsibilities, and the removal of access would have on the overall SOD violations for the organization. The simulation feature of the application allows the organization to play out the various scenarios to make the best business decision based on the simulation reporting.

21.9 PREVENTIVE CONTROLS

Preventive controls are a major selling point for all automated compliance software programs. For SOD, preventive controls translate to mean that the tool will provide real-time governance over the financial system and actively prevent system administrators or super users from granting themselves, and others, system access that is in direct violation of the SOD rules that the organization had previously defined. Often a notification will appear when a user attempts to violate

a SOD definition. Many applications have built in an approval mechanism where users may state their business need and a waiver or temporary access may be granted through the preventive control.

21.10 SOD RISK LIBRARIES

Several of the SOD tools come equipped with a risk library that an organization can use as a starting point to evaluate and customize the SOD definitions. These libraries are often based on best practices, and depending on the SOD application they may be ERP system specific and tied to specific application functions. Depending on an organization's approach to managing SOD efforts, the risk library can provide the organization significant time and cost savings. Not only does the library allow the organization to identify what risks may be prevalent within the organization, but it also allows for a quick deployment of SOD throughout the organization.

21.11 IMPLEMENTING A SOD AUTOMATION TOOL

The type of SOD tool an organization selects and the level of granularity at which it decides to set up the SOD rules will dictate the time investment and level of involvement needed from employees for implementation. Whether the organization is big or small, some universal activities are good practice to go through as part of the implementation.

One of the first steps to go through in the implementation process is to identify an implementation team that understands what the organization's business is as well as super users or key information technology (IT) employees who are familiar with the financial ERP system that is in place. Members should have an in-depth knowledge of the financial application and the ability to define which responsibilities can perform which functions, which becomes a difficult task if that knowledge is not present within your implementation team. This team of people will become the organization's decision makers and maintain and manage the SOD tool in the long run.

Depending on whether the SOD tool comes with a seeded risk library will determine the next implementation steps. Those applications that come seeded with a library of best practices or industry standards of SOD violations provide the organization a significant time-saving benefit. A key concept to keep in mind when setting up the SOD rules is that they should all focus on the risks that were identified for the organization. By working with the internal audit or risk management department, company-wide fraud risk assessments can be leveraged to help identify the areas of concentration in which SOD violation definitions should be created. By not taking a risk-based approach, the scope of the SOD violation definitions will dramatically increase. Also, taking a conservative view and identifying too many SOD definitions may potentially disrupt the flow of the business. A better approach would be to identify the key SOD violation definitions, clean up the user responsibilities to eliminate any false positive violations, and remove any unneeded access

that is granted in certain responsibilities. It is also important to note that many of these risk libraries offer only universal processes such as Order to Cash or Procure to Pay and do not examine processes unique to specific industries. Therefore, while the library provides an organization with an excellent starting point, more work will need to be completed to reflect the business of the organization and any other customized applications being used within the organization.

For those products that do not come with a seeded risk library, a risk library can be created and uploaded into the SOD application. One of the first steps is working with the local database administrator (DBA) or IT staff person to run a report in the ERP system to extract all the user responsibilities and the functions within the system. Based on the identification of SOD risks, SOD violation definitions will be mapped to the relevant responsibilities or functions. Although this activity can be time consuming, participants walk away with a clear understanding of SOD and often business process improvements result from the working sessions that are later implemented.

Once the SOD definitions have been identified and prepared for upload, business process owners and managers may review the conflicts to determine if any employees need to be waived from these SOD conflicts due to the nature of the job or the way the business is structured. These waivers can often be inputted at the user level or at the application responsibility level. Many products are also allowing a justification to be inputted next to waivers, providing clear reasoning to the auditors on why these employees are waived.

21.12 POSTIMPLEMENTATION SUPPORT

Once the automated SOD tool has been implemented, a couple of considerations should be kept in mind on an ongoing basis. The first consideration is that the ERP system does not remain static; changes are made to the financial applications, such as responsibility names may change, functions may change, and so on. It is important to keep that under consideration and perform a regularly scheduled review to ensure that the SOD violation library is kept up to date. Some SOD tools will aid in completing the review, while others will allow the definitions to become invalid. The second consideration is that job titles change and employees change; changes to the workforce occur, so it is important to check new job roles for SOD violations as well as maintain waivers. These items should become incorporated as part of the business processes and they will aid in keeping the SOD tool up to date and functioning properly.

Controlling user access to financial systems and ensuring the security of business information has become a hot issue for regulatory compliance; however, many of the automated SOD tools on the market aim to make this a painless task for an organization. After evaluating an organization's size and business, and going through the Segregation of Duties Consideration Checklist, the organization should be able to select the application that best suits its size and needs. Then the organization can enjoy real-time enforcement of SOD controls as well as reduced audit and remediation costs for years to come.

CHAPTER 22

INTERNAL CONTROLS BEST PRACTICES

Ian Rodgers

22.1 OVERVIEW

In its pure essence, a business exists to generate profits. The accounting and financial reporting disciplines within it allow the owners of the business and potential investors to value the business by inspecting those profits and evaluating the costs incurred in generating them. The business operations and risk management functions ensure that the firm conducts its processes in the most efficient and cost-effective manner. Without the assurances provided by internal controls over financial reporting, this assessment of profitability would be impossible. Without controls over operational risk management, that same investor has no assurance that this performance is sustainable. Finally, that same business has a legal and social responsibility to conduct its operations in a manner that conforms to generally accepted accounting principles (GAAP) and the various other prescribed regulatory constraints. Compliance-related controls enforce these rules.

As discussed in earlier chapters of this volume, therefore, an Enterprise Risk Management (ERM) model must address the enterprise's objectives with the following categories of control objectives:

- Planning—high-level planning, resource allocation, and budgeting
- Operational risk—day-to-day activities
- Financial reporting risk—presentation of financial results
- Compliance risk—adherence to statutory requirements of all jurisdictions within which the company does business

Put simply, the internal controls in each area ensure that the business is being run in accordance with the overall plan, that the financial statements and management reporting present an accurate view of the operations, and that all activities (including reporting) that are covered by statutory regulations are being carried out within the constraints of those regulations.

Let us take for example a major sales transaction (say 20 percent of sales for the quarter) that is intentionally counted twice in order to boost apparent profits, or a significant cost that is counted twice, thereby reducing apparent profits. (If the main criterion for the deception or error is to boost or reduce the level of taxable income, the same violations might be committed in reverse.)

It would be reasonable to expect that effective internal controls would either prevent such a transaction from being booked a second time or detect that the duplication has happened.

From a planning (sales forecast) perspective, a single transaction of this magnitude would be large enough to be identified by variance reports. Therefore, controls over the planning and forecasting process might identify this problem. In operational terms, controls to prevent this type of error or infringement would be an essential quality assurance provision. Clearly, double counting of revenue represents a considerable financial and management reporting risk and must be prevented by the appropriate internal controls over financial reporting. For all

of these reasons, the compliance imperative would necessitate that this policy violation be prevented or at least detected after the fact.

This chapter places its emphasis on financial internal controls since these are more easily scrutinized for discussion purposes than nonfinancial controls. However, most of the concepts encountered apply, just as effectively, to nonfinancial controls.

For example, in the United States, the compliance audit challenges raised by the personal privacy aspects of the Health Insurance Portability and Accounting Act (HIPAA)[1] regulations, which protect the confidentiality of communications between a health provider and the insured party, are similar to many of the compliance audit activities that resulted from the Sarbanes-Oxley Act of 2002 (SOX) (discussed in detail in a later chapter) over financial reporting for public companies.

(a) CONTROLS OVER PLANNING AND BUDGETING. In many respects, the governance process can be considered to start with the planning and budgeting activity. Internal controls over planning and budgeting are an essential aspect of both operational and compliance-related activities. Resource planning and revenue forecasting are the main benchmarks against which financial and management reporting are compared.

To continue with our example, in many organizations, the first indicator of this policy violation would be that the variance between the revenue forecast and the actual revenue numbers for that quarter would have been exceeded, or that the costs would be less than expected. In other words, either metric would be unexpectedly favorable. Whether this outcome would be considered a subject for cautious review or cause for celebration used to be a matter of management style. In these days of increased regulation, the cautious approach has become a necessity.

(b) CONTROLS OVER OPERATIONAL RISK. From a risk management viewpoint, an appropriate control to deal with the violations illustrated in our example would prevent an actual duplicate payment from being sent to the supplier concerned or the sale from being booked without strict review of the sales order originating the transaction. Since these are actual controls over the basic transaction flow, they would be considered operational controls designed to mitigate operational risk.

(c) CONTROLS OVER FINANCIAL STATEMENT RISK. To get back to our running example, the risk of the invalid sales or cost transactions in question, from a financial statement viewpoint, would be that the annual or quarterly results for the company would overstate revenue and understate costs. Thus there should be internal controls to prevent the infraction and, in the event of such controls failing, there should be internal controls to detect that a violation has occurred.

The emergence of the International Financial Reporting Standards (IFRS)[2] set by the International Accounting Standards Board (IASB) has simplified the dual-accounting issues faced by companies forced to operate under multiple Generally Accepted Accounting Principles (GAAP) regimes and raised the issue of

whether U.S. GAAP needs to exist as a separate entity from the accounting standards being adopted in the rest of the world. The differing interpretation of the framework according to the various regimes in Europe, Asia, Canada, and Australasia and the frequent need encountered within large, international companies to operate against both standards provides another challenge to the internal controls of an organization.

(d) COMPLIANCE-RELATED CONTROLS. The important distinction between compliance-related controls and their planning, financial reporting, and operational counterparts is that compliance controls are intended to demonstrate adherence to the associated regulation—so that the main outcome is the presentation of evidence to an auditor or external observer. From a compliance viewpoint, the emphasis is placed on the presentation of proof that prevention or detection has been effective and in the latter case that the control has facilitated eventual remediation.

In other words, the compliance-related controls are intended to provide the external observer with assurances that controls are in place to support the numbers that are published or, in the case of nonfinancial controls, to ensure that the company is fulfilling its obligations to the community as a whole and, from the point of view of the investor, will not face costly reprisals for noncompliance.

(e) THE AUDIT IMPERATIVE. While the concept of an external audit—carried out by an independent entity such as one of the Big Four accounting firms—is primarily a compliance issue, a company's own internal audit is subordinated to the review of all policies, including those intended to address operational efficiencies and management reporting. As such, when considering an integrated ERM internal controls regime, the ultimate test of those controls is the generic audit process, whether it be internal audit or external audit. As a result, this chapter makes no distinction between the two types of audit but treats the audit process as a generic validation of controls.

(f) REMEDIATION. When a control is found to be flawed, there is a requirement to correct the operation of that control and to correct (or remediate) any invalid transactions that may have resulted from that malfunction. Conversely, if the control is working correctly and has identified a number of control violations, the term *remediation* relates to the process of fixing those errors. This chapter concentrates on the implementation of controls and the audit of those controls and does not attempt to go into the intricacies of the remediation process. However, it should be noted that since prevention is not always possible, the difficulty of identifying policy violations, communicating the necessary corrective actions, and then tracking and communicating the ultimate resolution of the issues in question should not be underestimated.

(g) ENTERPRISE RISK MANAGEMENT, COSO ERM. Clearly the same types of mechanism that are implemented to enforce business rules for internal control and compliance may be subordinated to the purpose of promoting operational

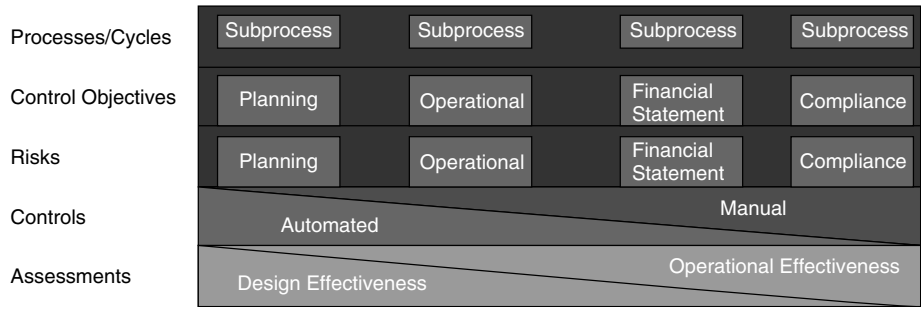


EXHIBIT 22.1 INTERNAL CONTROLS MODEL

efficiencies. Similarly, transaction monitors deployed for compliance purposes may be used to collect business intelligence to facilitate business process analysis and control. Almost all controls over financial reporting, furthermore, are relevant to planning, operational, and compliance risks.

The Committee of Sponsoring Organizations (COSO) model (discussed in detail in an earlier chapter) is based on the concept of control objectives. A control objective in the context of an implementation of internal controls might be represented as shown in Exhibit 22.1.

If we view a business as a collection of processes and cycles and further subdivided into subprocesses, a control objective is a mission statement for the effective operation of that process. For example, in an accounts payable department, a reasonable control objective might be to ensure that "supplier invoices are paid in a timely and cost-effective manner." Associated with each control objective is a risk that the control objective is not met satisfactorily and there are controls implemented to mitigate those risks which may be either manual or automated. Clearly, there is no purpose to implementing a control unless there is periodic testing to ensure that the control is effective, so the concept of a control assessment completes the model.

22.2 COSO II

The initial compliance regulations such as HIPAA and the Sarbanes-Oxley Act of 2002 (SOX) turned to the standards for internal controls proposed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission known as COSO I. In 2004 this organization sought to address the need for integration between compliance and business efficiency–related controls with its COSO 2004 standards (COSO II or COSO ERM).

While this chapter follows the general industry trend to relate the issues of internal controls over Enterprise Risk Management to COSO II, there is no intention to follow this standard; rather, it is used as a guideline where its structures are regarded as the de facto standard.

(a) ASSESSMENT OF CONTROLS

(i) Design Effectiveness and Operational Effectiveness. Under COSO I, an internal control must be evaluated against two criteria:

1. *Design effectiveness.* Is the control designed in such a manner as to prevent or detect a material policy violation and to satisfy the control objectives?
2. *Operating effectiveness.* Does the control operate as designed? Was it consistently performed, and was it operated by a person with sufficient authority?

Under COSO I, a control that fails either of these tests is considered to represent either a significant deficiency or a material weakness. The latter is more serious since by definition it could lead to material financial misstatement or an actual breach of the basic principle in question. A combination of several significant deficiencies may be construed as a material weakness.

Information technology (IT)-related controls have an especially sensitive position in this equation, since a single IT deficiency—say in user access controls—could potentially invalidate large areas of the internal control framework. It has been known for the entire compliance audit to fail as a result of a material weakness on general IT controls!

(ii) Scoping of the Audit Requirement. In deciding which systems should be included in an audit and, further, the priority that the associated controls should be given, two major factors must be taken into account: the *materiality* or level of risk of the process in terms of the likelihood that failure of a control will cause a significant violation of policy (or reduction in efficiency), and the *relevance* of the process, given that, though the quantities involved in a violation may be material, the impact on the business could conceivably be minimal. In terms of financial controls, a relatively large transaction may conceivably have little material impact on the financial statement.

For example, during the inception of SOX, a number of very astute accelerated filers realized that the controls over the inventory balance in the general ledger, in addition to the regular physical counts of inventory, reduced the criticality of the of the core inventory systems and subledgers. In this case these systems were deemphasized and sometimes excluded from the compliance audit.

(iii) Materiality. Only material events and material financial amounts should be considered. The problem here is that the concept of materiality differs between considerations of how a particular transaction impacts the numbers themselves and what it tells you about the business. For example, $3 million recognized as a result of employee fraud may be insignificant with respect to $600 million in profits worldwide but certainly tells you something significant about the running of the business as a whole.

At the time of writing, most firms have been working with materiality thresholds such that events with impact greater than 5 percent of gross profits or 10 percent of net profits are considered material.

(iv) Relevance. To some extent, this anomaly is addressed by a further principle, that of relevance, in that while not material, the fraud provision mentioned earlier would certainly be considered relevant. This principle, however, relates mainly to the opposite consideration, which is that even though numbers are material, they may be excluded from compliance considerations if not specifically relevant. For example, inventory numbers will always make a sizable contribution to a firm's balance sheet. If that firm's controls over its main financial systems provide adequate controls over the reporting of inventory numbers in the financial statements and the annual count can be proved to be accurate, there may be no need to implement additional controls over the company's inventory systems.

(v) Top-Down Approach to Controls Assessment. Amid the considerable controversy over the scoping of audits and the need to reduce burgeoning costs, the Public Company Accounting Oversight Board (PCAOB)[3] finally issued guidelines intended to improve the focus of compliance audits. The principle may be summarized in seven steps:

1. Identify and prioritize the principal disclosure risks—mainly top-level corporate controls such as period-end close.
2. Identify and prioritize the most significant financial statement accounts.
3. Identify the control objectives associated with these accounts.
4. Link these control objectives to the relevant underlying business processes.
5. Identify the risks associated with these control objectives.
6. Identify the controls that detect or prevent financial misstatements or fraud in these areas.
7. Make these controls a priority during the compliance audit.

This general hierarchical view presents a reasonable approach to achieving an efficient internal-controls architecture for any purpose. It is necessary only to replace the term *financial statement account* with the term *control parameter* to convert this into a generic statement that will apply to all four categories of internal control.

22.3 AUTOMATION OF CONTROLS

Clearly, internal controls must be implemented in the real world and these requirements have to translate into an appropriate combination of automated and manual controls.

Ideally, all possible controls would be automated. Manual intervention would be reserved for situations where the human factor helps to guarantee efficiency and/or accuracy. In practice, a control should remain manual only if the

relevant information is not available in the underlying systems, if it is presented in a manner that renders automated control impracticable, or where the cost of automation outweighs the benefits.

However, from an audit viewpoint, automated controls reduce the audit effort since they are inherently more reliable and may thus be tested using smaller samples. In fact, the latest PCAOB advice, on the benchmarking of controls, has made it clear that where a control is automated and it can be shown that this control has not changed between audits, there is no need to conduct detailed annual audits of that control.[4]

This leads us to a clear understanding of how a control should be viewed from an audit viewpoint. Where possible, a control should be automated to allow a minimum of auditing effort. Once automated, such a control should be monitored to demonstrate continuing effectiveness.

The same philosophy holds true for controls that relate more closely to the planning an operational controls. Wherever possible controls should be automated, changes to their configuration should be monitored and controlled, and there should be high-level corporate controls that act as police over the lower-level controls.

(a) PREVENTION VERSUS DETECTION. It will have been noted that frequently during our discussion the implementation of controls has been discussed in terms of prevention and detection.

In general, preventive controls influence user behavior by blocking invalid transactions or activities. It is usual for this to be effectuated by the implementation of checks that inhabit the user interface and prevent an invalid option or value from being selected. Alternatively, the invalid entry is allowed to be entered but is then rejected by an interim process before any damage can be done.

Detective controls do not seek to prevent policy violations. Rather, they seek to identify an invalid transaction in a timely manner to allow the infringement to be isolated and remediated.

Clearly, there is a fine line between the latter type of preventive control and a detective control. The only distinction is the timing that exists between identification and remediation.

(b) FIELD-LEVEL AUDIT. One specific type of detective control is the field-level database table audit. This is a rigid but unaffected form of control that simply tracks all changes to a specified field within the database. For example, if the company has a major risk concerning the yen/dollar exchange rate, changes to this field may be tracked by a field audit. In certain circumstances, this may be sufficient to mitigate a very serious risk.

In general, the control record here would show initial value of the field, final value of the field, date of change, and the ID of the user who made the change.

It should be noted, however, that the desirable nature of this type of control must be balanced against the cost of maintaining the data generated by this audit

trail and the inevitable system performance overhead of keeping track of all exchange rate changes.

It should also be noted that this example is a perfect illustration of a control for which neither the volume of the changes being tracked (currency codes and exchange rates are do not involve large amounts of data) nor the frequency of transactions would be cause for concern.

One factor that should be taken into consideration is that a field-level audit is not always optional. For example, in the context of the HIPAA regulations for the protection of personal privacy, it is necessary not only to show the status of a particular document but to show all retrievals of the document concerned. This is a good illustration of a scenario where a historical trail of changes would be highly desirable.

22.4 TYPES OF AUTOMATED CONTROLS

In general, the automated control system contains three elements: first, *access controls* that restrict access to the underlying business systems to ensure that only authorized individuals have access; second, *process controls* that restrict the activities performed by those users; and third, *continuous monitoring* that employs automation to detect, after the fact, system transactions, setup, or data changes that contravene corporate policy.

Each of these controls must be viewed with respect to business transactions, system setup, and business data since each of these elements must be secure in order to ensure valid internal controls. For example, each of these may be subject to access controls to ensure that only authorized individuals can view or change them. Similarly, process controls will ensure that only correct actions are taken on each and monitoring controls will track any invalid operations after the fact.

Let us take for example a set of automated controls whose primary purpose is to prevent an employee from entering a supplier invoice and then paying it himself. This control would prevent personal fraud perpetrated by an individual who had the ability to send a payment to a favored or nonexistent vendor. It would also prevent an individual from manipulating the numbers in the financial statement by booking incorrect or unauthorized expenses.

A user access control would prevent the user in question from being granted both the invoice and payment functions—segregation of duties (SOD).

A typical preventive process control would reside in the user interface of the payment entry screen and prevent the user from paying an invoice that he had entered himself. Note that from a user access viewpoint, this refinement would represent a mitigating control that fulfills the segregation of duties requirement.

A monitor would be run periodically to identify invoices that have been paid by the user who entered that invoice. This is an audit to verify the effectiveness of the process controls.

Note that in circumstances where that user interface controls impair or slow down the business process it is customary to implement the process controls in

detective mode. In this case, the control would be implemented as a detective but would prevent a violation by allowing the payment to be stopped before final confirmation.

(a) ACCESS CONTROLS. Access controls include basic user access grants (user provisioning) and the segregation of duties controls that ensure that the user cannot circumvent policy alone. For example, in the preceding example, an SOD control would prevent either one or other function from being granted to a single user, thus necessitating some degree of collusion for this invalid transfer to occur.

It is worth noting here another area where a judgment call must be made. One might conclude that even the ability to enter and pay an invoice is a marginal risk given that the individual in question cannot himself set up a supplier in the system. In this case, we might decide that this access constitutes an SOD conflict only if the user also has access to enter or update a vendor in the system concerned.

Another key element of efficient access controls is the ability to link the systems user to the entry in the human resources system such that privileges cease when an employee is terminated and access is reviewed when the employee job function changes.

(b) PROCESS CONTROLS. Process controls can be categorized in terms of three intrinsics: *recognition*, *measurement*, and *timing*—meaning control over what is being captured, how much of it is being captured, and when (as in which financial period) it is being recorded.

In our example, the process controls would identify the fact that both an invoice and a payment had occurred, would establish that the amounts concerned are material, and would identify the financial period (say, month) to which the infringement, and therefore the risk, relates.

(c) CONTINUOUS MONITORING. Whereas process controls may be either detective or preventive, monitoring controls take effect after the fact and as such are exclusively detective. As a result, monitoring controls are sometimes synonymous with their equivalent detective process controls. The difference is in the purpose and deployment of the control concerned.

Detective process controls are principal controls that ensure correct operation of a business process. Monitoring controls are historical. For example, a control that checks payments to ensure that there is no duplication before a bank transfer has been finalized is a detective process control. The same control run every quarter to do the same thing is very much a historical monitor.

As stated earlier, a monitor can track the status of transactions, system setups, or specific data elements. In the example, a monitor can be used to demonstrate that there have been no duplicate payments (transactions), may show that the payment types (setup) have not changed, and may show that the bank account numbers (data) have not changed—thus supporting the conclusion that duplicate payments have not occurred.

There are very specific areas, however, where monitors can deliver benefits that access and process controls cannot deliver. These areas primarily concern the tracking of business analytics and key performance indicators. Such controls are necessarily historical and add value through additional analysis.

An example of this is a monitor that tracks the days sales outstanding[5] (DSO) metric for a sales organization. This metric provides a measure of the average number of days that it takes to collect from the firm's debtors and is a calculation that involves the total receivables accrued over a period, the total sales for that period, and the total collections during that period. From a compliance viewpoint, this is an essential metric since it indicates scenarios where a bad debt reserve may be necessary. Similar monitors are best practice for any key performance indicators required to back up judgment-based accounting entries.

As discussed earlier, automated controls may be preventive or detective. In this context, monitors are detective applications designed to demonstrate the effectiveness of the underlying controls. It will come as no surprise that often detective controls and monitors are actually the same controls, the difference being that they are deployed with differing objectives in mind.

(i) Control Areas. Having established the types of controls that are required for risk management purposes, the question becomes: "What do we need to control?"

Whether viewed from a business or information technology viewpoint, the answer should be obvious:

We have to ensure, first, that *transactions* are protected—that the actual actions performed by the user are recorded accurately and not subject to corruption after the fact; second, that the *master data* held in the system remains accurate; third, that the underlying *system configuration* is protected. To continue with our example, we need to ensure that the invoice data is accurate and compatible with business policies, that the user is using a valid supplier, that the supplier data is accurate, and that the standard setups—for example, the currency for the accounting book concerned—has not been modified in such a way that the transaction is compromised.

The following example should provide a reasonable summary: Those of us familiar with accounting principles will recognize the fact that an organization is liable to pay for goods that have been received regardless of whether an invoice has been received from the supplier. This processing of so-called un-invoiced receipts can be a very significant activity for some organizations, and the omission of such liabilities from the financial statement may be highly suspect or even be considered fraudulent.

(d) TRANSACTION CONTROLS. In this scenario, a necessary transaction control would recognize that a receipt of goods had not been invoiced and may automatically create an accounting journal to recognize the liability. (Let us say, for example, that the creation of this journal is optional and determined by a

"accrue un-invoiced receipts" check mark selected during the setup of the receiving function within the system.)

(e) MASTER DATA CONTROLS. To continue the example, if the item being received is a major fixed-asset purchase such as a piece of plant or equipment, it may be necessary to recognize the liability immediately so that it is visible in the books from day one, whereas smaller inventory purchases might be accrued at month-end.

In order for this distinction to be made, the system master data must accurately describe the item concerned, so that the appropriate processes will run.

Master data controls would protect this classification and ensure that it is not compromised.

(f) SYSTEM CONFIGURATION CONTROLS. In this example, it would be necessary to protect the "accrue un-invoiced receipts" setup option to prevent it from being disabled or to detect the fact that it had been disabled.

Clearly, the worst possible scenario would occur if this option were disabled without the knowledge of those responsible for the financial statements. In this case, the business community would believe that these costs were being recognized, while in fact the financial statement would be showing the liabilities without this component.

(i) Accounting, Consolidation, and Financial Reporting Controls. Although they are clearly an aspect of the process controls, general ledger (GL) controls are worthy of special consideration.

In general, the financial statement is produced from the main financial ledger or general ledger. Often the final numbers are massaged in a financial consolidation tool such as Hyperion or even in a spreadsheet, but the raw numbers originate in the general ledger.

The vast majority of source transactions, however, take place in subsidiary ledgers that are a direct representation of the transactions concerned. For example, the revenue numbers reported in the financial statements are taken from the GL, but the sales transactions discussed earlier in this chapter and the proposed controls over them would probably be implemented in the accounts receivable and order management systems. Normally the results of operations are posted directly from the subsidiary ledgers to the general ledger from whence the financial statements are generated.

Whereas accounting department activities within the general ledger are often detail-oriented transactions, from a risk management viewpoint it is more instructive to consider the general ledger, and any associated consolidation and reporting systems, as the core repository for financial reporting and to consider this as the process that incorporates the basic controls over accounting entries: namely, which numbers are being booked and by whom.

The key controls from a general ledger viewpoint may be summarized as:

- Automated reconciliation between GL entries and the equivalent subsidiary ledger entries—for example, between the total invoices entered in the payables ledger and the total monies owed for that period in the general ledger (balance sheet), and similarly, total sales booked in the receivables ledger and the total monies recognized as future receipts from customers in the general ledger.

  These numbers are reported in the financial statements as, respectively, liabilities or assets of the company and form a major part of the information that a potential investor would use to evaluate financial performance.
- Controls to prevent unauthorized material entries to specific financial statement accounts. As stated before, the vast majority of activity that hits the financial statement occurs in subsidiary ledgers that are intimate with the transactions concerned. For example, a write-off of obsolete inventory would be performed in the inventory subledger by an inventory manager who is intimate with the material concerned. Where the entry is made directly in the general ledger, controls are required to ensure that these are properly authorized. The inventory write-off mentioned earlier, to continue our example, might be entered directly into the GL by the finance department but may be routed to the inventory manager or vice president of materials for approval.

(ii) Subsidiary Ledger Controls. Having singled out general ledger controls for special consideration, it is as well to make the distinction between these controls and controls over the subsidiary ledgers that track detailed-level operational transactions. While the general ledger tracks the financial health of the business at the high level, the status of individual transactions or groups of transactions must be monitored or controlled within the subsidiary ledgers. For example, although the Basel II regulations are clearly intended to identify and control the financial exposure of a trading organization, which should be apparent in the GL, the main controls need to be over individual transactions, transaction types, and off-balance-sheet transactions, which can be managed in detail only in the organization's trading systems, which feed their numbers into the general ledger in summarized form.

The same would also be true of supply-chain risk, for which a manufacturing organization would need to maintain controls over its inventory subledger.

Further examples of subsidiary ledgers include accounts receivable, accounts payable, payroll and human resources, and fixed assets. The control examples that follow provide more specific illustrations of controls in these areas.

22.5 PRIMARY FINANCIAL CONTROL CONSIDERATIONS

While organizations differ in the overall profile of their businesses and the associated risk and control priorities, the early experience of the Sarbanes-Oxley accelerated filers and the weaknesses reported thereof have provided substantial

guidelines as to the areas of an organization's operations and financial reporting that offer the greatest opportunity to control risk.

This section reviews some of these high-risk areas. It is as well to note that, where intent has been determined, some violations have resulted in serious prosecutions.

Clearly, the specific controls to be employed by a given organization are too varied to be detailed here; the following, however, are representative samples of the types of control issues that have caused significant problems for organizations embarking on 404 certification for the first time. Consequently, the specific controls relate to risk management from the point of view of a publicly traded company that is subject to U.S. GAAP and is listed on one of the U.S. stock exchanges. In almost all cases, however, the provisions discussed are relevant to any company in any jurisdiction, whether privately owned or publicly traded.

Note that no attempt is made here to identify individual segregation of duties violations; rather it is assumed that any key control is subject to the prerequisite that sufficient segregation of duties constraints are in place to allow the control to be effective.

(a) REVENUE CYCLE. The activities that occur from the booking of sales orders (or service commitments) to the receipt of customer payments are listed below. This will usually include customer account analysis, customer credit, collections, and the soft customer account management activities.

Significant Control Elements

- Price lists must be correctly authorized. Changes should be routed for approval by a responsible party.
- Revenue is recognized within correct periods where ownership of goods has been transferred to the customer or services have been delivered in accordance with contractual terms. Controls should be put in place to ensure that revenue is not recognized at point of shipment where policy dictates that it should be recognized at destination.

  Note that the emphasis here is placed on the prevention of recognition at point of shipment rather than the proof that shipment has reached its destination—which presents many more logistical challenges. However, it should be noted that most of the major courier companies offer electronic confirmation of shipment, which may reasonably be built into a control, provided that transaction volumes and logistics will allow it.
- Deferred revenue such as maintenance contracts should be correctly amortized in the appropriate periods. In particular, controls must be in place to prevent such transactions from being recognized as a single-revenue event.
- Returns from customers are correctly authorized and are for quantities consistent with the original sale. An approval work flow would suffice.

- Warranty reserves are adequate and are consistent with agreed reliability metrics. Since this is a judgment-based metric, a satisfactory automated control would compare the actual amounts reserved to a benchmark derived from a suitable test of reasonableness—say a multiplier applied to sales for the period.
- Bad debt reserves are adequate and are consistent with the metrics methodology agreed to estimate potential defaults.

(b) PROCUREMENT CYCLE. The activity that occurs from the entry of a purchase requisition, purchase order, supplier contract, or any purchase commitment undertaken to the generation of a payment to the supplier is listed below. This will usually include the review and approval of suppliers as well as the soft supplier management activities.

SIGNIFICANT CONTROL ELEMENTS

- Purchase orders must be approved by a responsible individual and form the basis of the firm's estimate of contractual obligations.
- Capital expenditures such as fixed assets, construction, and research and development must be recorded correctly. Controls must be in place to prevent disposables and other noncapital expenditures from being recorded as capital expenditures.
- Payments must be correctly authorized. Controls should be in place to prevent incorrect recognized expenditures and fraudulent payments. For example, purchases that source costs of goods sold should be recorded in the same period as the sales concerned.

(c) INTANGIBLES. Goodwill, patents, licenses and any other intangible items on the balance sheet are listed below.

SIGNIFICANT CONTROL ELEMENTS

- Ensure that Financial Accounting Standards Board (FASB) and IFRS rules for testing of impairment are adhered to. Often a discretionary approach is taken to adjustments. This is no longer acceptable. In a large organization, controls must be in place to prevent this, especially where the entry is being made according to local GAAP in an international affiliate where discretionary adjustments may be acceptable.

(d) PROPERTY, PLANT, AND EQUIPMENT CYCLE. All activity relating to the management of long-term tangible assets including initial capitalization, depreciation, and retirement is listed below.

SIGNIFICANT CONTROL ELEMENTS

- Ensure that only genuine fixed assets purchases or construction costs are recorded in this category and that expenses are not misclassified as fixed assets or construction in process.

- Ensure that depreciation is carried out according to the correct method, using the correct expected life for that asset.
- Ensure that adjustments are authorized and consistent with the appropriate GAAP or reporting standards.
- Ensure that disposals are correctly accounted for and that depreciation is adjusted appropriately according to the appropriate tax conventions. Also, care should be taken to manage the dual accounting controls where fair value methods are applied that differ between jurisdictions within which the company operates.
- Material impairments should be identified in a timely manner. Where an impairment is sufficiently large to constitute an event reportable to a regulatory authority, a notification should be routed to the responsible party.

(e) INVENTORY/PRODUCTION CYCLE. All activity that occurs from the receipt of an item or subassembly to its consumption in the manufacture of finished goods inventory. This activity includes all aspects of supply chain planning. The accounting for labor absorption and ongoing "construction-in-progress" are also essential elements.

SIGNIFICANT CONTROL ELEMENTS

- Access and updates to inventory item master files should be controlled to ensure that item definitions and costs are not manipulated inappropriately.
- Scrap, write-offs, and write-downs should be strictly controlled since these impact the bottom line directly. Care should be taken to ensure that these transactions are correctly authorized and controlled. Reportable events should be routed to a responsible party.
- The assessment of reserves must be supported by suitable metrics for shrinkage and other impairment. Those elements of the system that support these metrics should be subject to appropriate internal controls.
- Adjustment to inventory item costs and bills-of-materials or work-in-process entities should be strictly controlled to avoid fraudulent manipulation of costs.
- Physical inventories and cycle counts should be fully authorized and subject to reasonableness reviews at the company/entity level.
- Returns/RMA/RTV quantities should be subject to internal controls that ensure that returns do not exceed the amount of the original order.

(f) HR/PAYROLL CYCLE. These processes include all elements of the "hire-to-retire" cycle and incorporate payroll and benefits processing.

SIGNIFICANT CONTROL ELEMENTS

- The system should offer verification that employees and new hires are qualified for the jobs that they hold, especially in areas that impact on

risk or compliance such as finance. One frequent occurrence is that doubts have been cast as to the accuracy of financial reports when a key member of the team has been found to have misrepresented his or her experience. In the event that this should occur, it must be possible to track the actions and transactions performed by that individual.
- Ensure that payroll is correctly authorized and subject to appropriate segregation of duties.

(g) EQUITY CYCLE. Processes that impact on the equity section of the balance sheet, including treasury activities and employee stock options are listed below.

SIGNIFICANT CONTROL ELEMENTS

- It is essential that any expense associated with the allocation of an employee stock option (ESO) grant is correctly recognized and that measurement methods and timing are applied appropriately.[6]
- It is essential that employee stock holdings are tracked to ensure that the organization is aware of which employees are subject to the Section 16 insider trading regulations. This tends to vary over time. The organization must, however, disclose these individuals and process tax liabilities accordingly.
- Controls should be in place to ensure that regulatory constraints over the magnitude of hedge transactions (for example Financial Accounting Standards Board No.133 (FAS 133)) are taken into account and that positions are evaluated with sufficient accuracy to ensure that the scenario is an effective hedge for the underlying transaction. In addition, any speculative element is within the allowed margin for the trade concerned. Of particular interest are purchase or sales contracts with a built-in derivative component.
- Confirm that the beneficiaries of ESO allocations are genuine employees.
- Ensure that stock allocations do not exceed the planned amounts improved by the compensation committee.
- Confirm stock prices and volatilities used in fair market value calculations.

(h) FINANCIAL CLOSE AND REPORTING CYCLE. The list below includes general ledger activities, subsidiary ledger reconciliation, consolidation, and financial reporting. Significant elements include budgeting as well as intercompany and foreign currency processes.

SIGNIFICANT CONTROL ELEMENTS

- Ensure that manual journal entries are reviewed and approved.
- Ensure that period close within each ledger is approved.
- Ensure that recurring journals, accruals, and reversals are reviewed and approved during each period.

- Provide the means to track fluctuations in key accounts between periods.
- Provide the means to track key performance indicators such as gross margin between periods.
- Enable the tracking of reportable events such as material write-offs, impairments, or provisions.

(i) TAX CYCLE. Processes that relate to corporate taxes including income tax and sales taxes (sales, use tax, and value-added taxes) are listed below. These activities help the organization to run its business in a tax-efficient manner while ensuring timely and accurate tax reporting.

SIGNIFICANT CONTROL ELEMENTS

- Ensure that income tax provisions are accurately recorded, especially with respect to online sales and sales impacted by unusual provisions for a given country or state.
- Provide controls to ensure that critical data such as geographical location and tax jurisdiction are complete and accurate.
- Provide tests of reasonableness to validate the accuracy and timing of tax payments.
- Provide tests of reasonableness to ensure that tax reserves are accurately reported.

(j) LEGAL CYCLE. Listed below are activities that help to ensure that the organization conducts its business according to the established legal policies. These requirements pervade the full spectrum of a company's activities. These examples consider only the practical protection of printed contractual terms.

SIGNIFICANT CONTROL ELEMENTS

- Implement controls to ensure compliance with contractual terms—for example, that the terms and conditions on purchase orders or customer invoices are fully secured and that any changes are audited.
- Implement controls to ensure that data that relates to export, customs, and the transfer of ownership are fully-secured and subject to an effective audit trail of changes.

22.6 COMBINING COMPLIANCE AND OPERATIONAL REQUIREMENTS TO ACHIEVE AN ROI ON COMPLIANCE EXPENDITURE

Clearly the same types of controls that are implemented to enforce business rules for compliance may be subordinated to the purpose of implementing controls that promote operational efficiencies. Similarly, a control deployed primarily to monitor transactions for compliance purposes can be used to collect business intelligence to be used as a baseline for analysis and process improvement purposes.

Whereas process improvement controls tend to be incorporated into the natural flow of a business, their compliance-related counterparts are often less well integrated adjuncts to a process that functions more smoothly without them.

If we consider the relationship between the routine period-end financial processes—those that involve consolidation and reporting of the main financial statement while reconciling and adjusting the underlying transactions—and those activities that are subordinated to the compliance burden, the stratification of activity and objectives is apparent, as shown in Exhibit 22.2.

Note also that, in this scenario, remediation of policy violations is primarily managed as a manual process or project with no specific framework offered by the underlying systems.

The business process is a continuous cycle that lends itself to automation and streamlining, whereas the compliance task is discontinuous, project-oriented, and subject to time-consuming manual exercises that make it impossible to incorporate best-practice business efficiencies.

Conversely, where the compliance tasks are embedded in the basic business flow, as shown in Exhibit 22.3, it is possible to streamline the whole process to reduce costs and to deliver the business benefits of a fully integrated application and controls platform. In this scenario, remediation can be facilitated by a framework of alerts and notifications to ensure that the appropriate individuals are notified of policy violations and to coordinate any transaction sample and test requirements that have been agreed on with the auditors; similarly, a set of

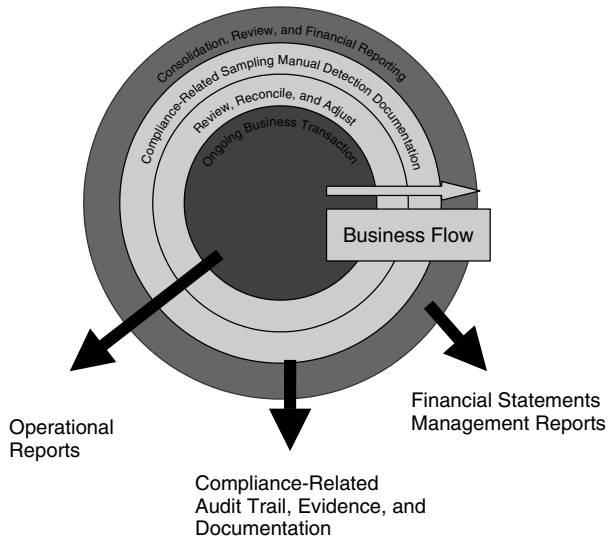


EXHIBIT 22.2 COMPLIANCE PROCESSES TREATED AS A STAND-ALONE PROCESS

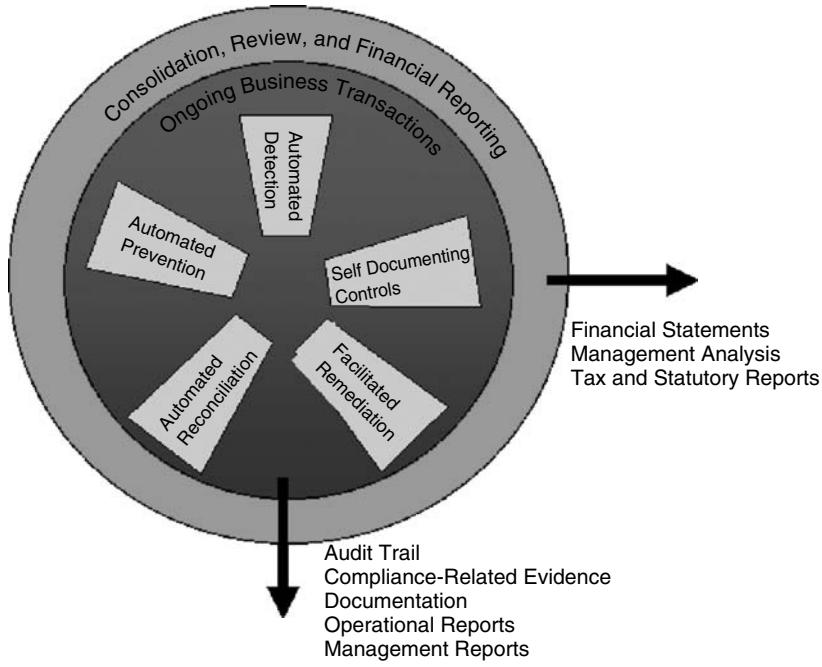


EXHIBIT 22.3 COMPLIANCE-RELATED PROCESSES EMBEDDED WITHIN CORE BUSINESS PROCESSES

reports will be provided to supply evidence of remediation. In addition, automated controls are usually self-documenting, thereby reducing the effort required to maintain spreadsheets or to construct evidence from disparate sets of listings.

(a) PRACTICAL CONSIDERATIONS. If this type of integration is to be achieved, the following prerequisites must be met:

- *Obtain full buy-in from all stakeholders.* It is a curiosity that in one organization, the finance stakeholder sees all things as possible and demands automation that appears impractical to the IT management. In another, the same control may be considered a pie-in-the-sky approach by the finance team while the IT stakeholder might see it as a key path to achieving business benefit. In either scenario, the internal audit functionaries may fall into either camp. The truth is that each automated control scenario must be considered on its merits and costs, and that practical benefit can only be achieved if all parties show a commitment to the automation of controls.
- *Design best practice controls.* Start with an "in an ideal world" approach to design. Then subordinate this design to the practical constraints. If design is conducted the other way round, the controls will always falls short of the business requirements.

- *Be prepared to implement process changes and additional integration between systems.* Assess the need for the revision of business processes to support automation and integration. This may require additional integration between systems and/or the modification of key process flows.
- *Assess the quality and usability of the underlying data in the context of each control concerned.* The basic principles of garbage in, garbage out still apply. If the data are not available to support a particular control, it is destined to fail, however well designed.
- *Take a phased approach to the implementation of automated controls.* In most organization, the access controls and SOD are addressed first. Preventive and detective mitigating controls for SOD are a logical next step, and since these are effectively process controls and/or monitoring controls, they lead directly to the implementation of more general automated controls. Finally, the sophisticated Key Performance indicator (KPI) and business efficiency control monitors may be implemented. It should be noted that although these controls are firmly within the business efficiency category, they are often also very fundamental controls from a compliance viewpoint.

It has been the experience of organizations that have taken this path that embedded controls yield real benefits in terms of reduced audit costs and improved business efficiencies. The approach also sets the organization on a path that facilitates the streamlining of business processes and a flexible controls infrastructure that is responsive to change, whether that change is the result of government regulation or changing market conditions.

22.7 FURTHER CONSIDERATIONS

(a) COMPANY-LEVEL CONTROLS AND THE CONTROL ENVIRONMENT. The COSO framework makes provision for two levels of control, *company-level* controls that reflect the overall control architecture of the organization and the more granular *process-level* controls that have formed the bulk of this discussion so far. Company-level[7] controls include first, the control environment—the culture, integrity, and efficiency of the organization—and second, the controls that provide financial oversight such as the period-end close, independent analytics, high-level control monitors, and overall corporate performance metrics.

Often, company controls can identify problems that occur at the process level, and the PCAOB goes as far as to suggest that where a company-level control will suffice to provide the appropriate assurances, it is not necessary to audit the process-level controls. (Note that the process-level controls might be necessary—but need not be audited for compliance purposes.)

The emphasis on culture, integrity, and a raft of other intangibles makes this type of control unwieldy in the context of this chapter, and it seems unlikely that any real benefit will be gained by delving more deeply into the subject. However,

the author acknowledges that the concept is one that must be taken very seriously by the practitioner when implementing an internal controls regime.

(b) INTERNATIONAL CONSIDERATIONS. While companies in the United States are still largely governed by traditional U.S. GAAP considerations, the rest of the world has converged toward the International Financial Reporting Standards (IFRS),[8] set by the International Accounting Standards Board (IASB). As a result, there is substantial convergence between the format of internal controls implemented by organizations in Europe and the rest of the world. Ironically, this convergence provides a manageable focus for accounting treatment differences between the United States and the rest of the world and it is possible to opine, therefore, that the issues discussed within this document may be considered relevant to both sets of standards.

(c) CobiT. As has been stated several times within this volume, the COSO standards revolve around the concept of defined control objectives for an organization. Where those control objectives concern information technology, however, a more detailed set of guidelines is required. The standard most frequently adopted in this regard is the CobiT[9] standard (Control Objectives for Information and related Technology) established by the Information Technology Governance Institute (ITGI).

The CobiT view of the implementation of a system's infrastructure may be summarized as:

- Plan and organize
- Acquire and implement
- Deliver and support
- Monitor and evaluate

While detailed discussion of these phases is well outside the scope of this volume, it is well to note that within the overall spectrum of the implementation of internal controls, there is an IT infrastructure that supports these controls and must, itself, be subject to stringent controls and compliance imperatives.

22.8 CONCLUSION

The business environment and compliance landscape continues to evolve, and while there is little doubt that the period during which this chapter was written constitutes a significant watershed in the development of national and international business models and regulatory standards, it is important to note that this change is an essential and healthy aspect of the internal controls ecosystem.

The secret to the implementation of an effective internal controls strategy, therefore, is to ensure that the fundamentals are in place and that these are implemented in a manner sufficiently flexible to respond to inevitable change.

Ideally, the efficiently run organization develops effective internal controls as a matter of course. The role of the audit and internal controls practitioner is

to facilitate the evolution of these controls to match the changes in the business and regulatory environments.

It is the aim of this chapter to provide a baseline for the environment as it currently presents itself and to suggest best practices to accommodate it. It is hoped that this will provide the reader with some initial guidelines to help overcome the various challenges presented by the implementation of effective internal controls.

Notes

1. Health Insurance Portability and Accounting Act of 1996 (see www.hippa.org).
2. Public Companies Accounting Oversight Board (PCAOB). Found at www.pcaob.org.
3. PCAOB AS2, 2005 Roundtable, December 19, 2006, recommendations.
4. Ibid.
5. Calculated as Days in Period × Total Outstanding Receivables/Total Sales during Period. Typically, the period is 91 days.
6. Mandated in the United States by FASB 123, which has been the basis of innumerable prosecutions by the SEC. The IASB standard is defined by IFRS 2.
7. Ibid.
8. Summaries of the International Financial Reporting Standards found at www.iasb.org.
9. Control Objectives for Information and related Technology (CobiT). Details found at www.isaca.org (see Chapter 11 — IT Governance Overview).

CHAPTER 23

IT CONTROLS AUTOMATION AND DATABASE MANAGEMENT: DEFENDING AGAINST THE INSIDER THREAT

Harald Collet

Driven by regulatory pressures, internal auditors have become savvy in designing and testing controls for information technology (IT) operations, which has resulted in a tremendous burden on corporate IT departments to respond effectively. On this backdrop, most organizations must take a fresh look at ways to drive IT controls automation to manage costs and develop a more effective long-term IT controls environment. This chapter focuses specifically on ways to implement effective automated preventive and detective controls for database management as well as strategies for securing these critical repositories that underpin most organizational back-end processes and applications. Implementing automated internal

controls on database management provides operational benefits and can lower the ongoing cost of compliance.

23.1 THE NEW INTERNAL CONTROLS ENVIRONMENT: IT DEPARTMENTS FACE A SEA CHANGE

After a few years of uncertainty and turmoil, a majority of large organizations now have a good grasp of the new regulatory requirements and the impact on processes and systems. The uniform response has been to implement stringent internal controls and to empower internal auditors to become much more aggressive in auditing internal processes and the supporting IT processes and systems. In turn, the impact on IT departments has been a dramatic increase in the labor costs and amount of IT budget tied up in projects driven by internal audit requirements.

Case in point: IDC estimates that IT spending on compliance infrastructure software solutions exceeded $5 billion in 2006 alone, with a breathtaking compound annual growth rate (CAGR) of 18.4 percent through 2010.[1] Another study, conducted by Gartner Research in 2006, found the typical IT organization spends between 5,000 and 20,000 hours annually on reaching Sarbanes-Oxley Act (SOX) compliance. And IT organizations at smaller companies spend as much time on SOX compliance as those at larger companies. The survey also revealed that a shocking one-third of audit deficiencies under SOX relate to IT.[2] While companies may have made headway on translating policies into technical controls, the effectiveness of these controls is being questioned as never before.

This focus on controls effectiveness forces organizations to evaluate IT controls to lower the risk of malfeasance. Nonetheless, a PricewaterhouseCoopers survey in 2006 of more than 7,000 executives and IT directors in more than 50 countries found many organizations still ignore the risks of noncompliance with critical data security and data privacy requirements.[3] The survey data also highlights that the level of compliance with data privacy mandates is not just a North American issue; international organizations are also struggling to implement the appropriate data security and privacy safeguards to address requirements such as those imposed by the European Data Privacy Directive and the forthcoming Japan Corporate Governance Act. (See Exhibit 23.1.)

The key challenge facing most IT organizations when responding to the internal audit requirements is the mix of costly manual and compensating IT controls that have been deployed to pass initial audits in the first few years. The costs of this approach, however, can be staggering. In one IDC study, an average midmarket publicly listed enterprise is expected to spend in excess of $600,000 on IT-related manual controls (924 man-days at $500 loaded cost/hour) in year one alone.[4] In their calculations, IDC expects this IT-related cost to rise slightly in following years if no steps are taken to automate the labor-intensive manual IT controls.

One particular area of technology safeguards that often receives only cursory attention and has been addressed with a hodgepodge of manual and

U.S. organizations still ignoring security and privacy laws . . .			. . . but international colleagues are negligent as well.		
Percentage of U.S. organizations admitting they need to be in compliance with a specific law but are not	2005	2006	Percentage of non U.S. firms admitting they need to be in compliance with a specific law but are not	2005	2006
California security breach notification law	15%	18%	Australian Privacy Legislation (Australia respondents)	48%	50%
Sarbanes-Oxley	38%	35%	CIVIL (France respondents)	35%	42%
HIPAA (health-care respondents only)	38%	40%	Data Protection Act of 1998 (UK respondents)	24%	31%
Gramm-Leach-Bliley (financial services respondents only)	17%	14%	European Union Data Privacy Directive (Europe respondents)	45%	45%
Other state/local privacy regulations	10%	29%	Canadian Privacy Act (Canada respondents)	38%	30%

Source: "The Global State of Information Security 2006," PricewaterhouseCoopers (www.cio.com).

EXHIBIT 23.1 FAILURE OF U.S. AND INTERNATIONAL ORGANIZATIONS TO ADDRESS DATA PRIVACY MANDATES

compensating IT controls is database management. Indeed, the relational database system may be the last frontier for IT controls and is now coming under close scrutiny since the risks of fraud and misuse are very real. Consider the pick-six scandal in 2002, where a database administrator (DBA) was able to defraud the New York Horse Racing Association out of $3 million. In this particular instance, the rogue DBA accessed a lottery database containing data on the winning horses in each race. The administrator took advantage of his proprietary access to this database and the time-delay in reporting horse-racing winners to falsify tickets purchased by an accomplice.[5]

Certainly, companies ignore the threat of an evil insider at their own risk. Forrester Research found that company insiders committed 65 percent of security breaches while only 25 percent of companies detected those breaches.[6] Another study, by the Burton Group, found that security tools focused on external security threats to IT systems fail to catch insiders, whose frauds account for 80 percent of the losses in the average organization.[7]

When it comes to the most sensitive data within an organization, super users and DBAs often hold the keys to the kingdom, and the consequences of ignoring the risks associated with this gap in IT controls can be severe for any organization.

23.2 A LAYMAN'S GUIDE TO THE ROLE OF RELATIONAL DATABASE MANAGEMENT SYSTEMS IN AN ENTERPRISE

Record keeping is an important aspect of most every business, and much of the world's computing power is dedicated to maintaining and using databases that contain vast amounts of enterprise data. Most business users never work hands-on with a database, but an elementary understanding of the role of enterprise databases is critical to assess the appropriate IT controls environment.

At the most basic level, a database is a place where you can store data and then arrange that data easily and efficiently. All kinds of data, from business-critical financial data to records of sales, employee data, e-mail, and customer information are stored in some form of a database. In particular, a relational database is a database that conforms to the relational model, and strictly speaking, is merely a collection of relations (frequently called tables).

Most large organizations run many different instances of Relational Database Management Systems (RDBMS), which are software packages from large software vendors such as Oracle, Microsoft, IBM, and many others. For modern computing systems, RDBMS is the preferred method of storage for multi-user applications, where coordination between many users and processes is needed. The success of the relational database model is partly due to a set of flexible open standards defined interfaces and programming languages (SQL) that allows administrators to manage and share the data efficiently.

The *openness* of this environment is also a potential Achilles heel from an IT controls perspective, since it offers administrators and applications many different ways of accessing the data with few built-in controls. In some ways the characteristic that successfully made the RDBMS the operational IT foundation of modern businesses is now coming back with a vengeance to haunt IT departments. Forrester Research, for instance, estimates that the average database boasts 30% more user accounts than it really needs, largely because of inactive and duplicate accounts created by DBAs looking to avoid frustrating business users demanding access.[8]

In the past, most organizations have been lax about addressing these vulnerabilities using the built-in security capabilities in the RDBMS due to the—real or perceived—difficulty and computing processing overhead associated with the use of this security functionality. Instead, many organizations have focused on manual or compensating controls to demonstrate the security of their data during audits. But the labor cost of the manual IT controls approach has often stretched IT budgets to the limit.

More than ever, companies of all sizes face challenges around controls automation for databases. But larger organizations in particular are facing a considerable challenge, since they often run more than 1000 database instances and sometimes employ hundreds of Database Administrators (DBAs) in their IT departments. For these larger organizations, controls automation has taken on

even more urgency as internal auditors are pressing for more automated controls environment to raise the effectiveness of the overall environment.

23.3 A LAYMAN'S GUIDE TO THE ROLE OF THE DATABASE ADMINISTRATOR IN AN ENTERPRISE

The role of the DBA within the IT department is critical to running almost any large modern enterprise, and the DBA workforce is a carefully safeguarded competitive IT asset. Traditionally, the DBA is responsible for the environmental aspects of the databases that underpin critical business processes and applications.

The typical environmental tasks include:

- Integrity—verifying or helping to verify data integrity
- Availability—ensuring maximum up time
- Recoverability—creating and testing backups
- Security—defining and/or implementing access controls to the data
- Performance—ensuring maximum performance, given budgetary constraints
- Development and testing support—helping programmers and engineers to efficiently utilize the database[9]

Typically, a DBA has unfettered access to all production data contained within databases in an organization regardless of the sensitivity of the data. To put it on point: DBAs have access to sensitive quarterly financial data before chief financial officers do. To be sure, most organizations conduct various forms of background checks on their DBA staff and have some form of detective and preventive controls in place, but the basic fact remains—the DBAs have the proverbial keys to the kingdom (in this instance sensitive information) without an effective system of checks and balances.

Increasingly, organizations are now looking to implement different forms of segregation of duties for DBAs within their IT departments to address regulatory requirements, but often struggle with the actual implementation of policies without hindering the effective work flow of DBAs. Some organizations take an approach where more junior DBAs may not have access to critical production databases or have to go through a "submit-commit" cycle with a secondary senior DBA signing off on any production system changes. Alternatively, controls can be built directly into the kernel of the RDBMS by the software vendor to ensure that DBAs do not have access to view or copy the actual data, but can maintain and operate the database environment nonetheless.

Operationally, the average DBA faces a complex environment that includes supporting heterogeneous database platforms and supporting stakeholders from various lines of business. As soon as an issue arises, DBAs are called upon to fix them under great time pressure since system downtime or scalability bottlenecks can cost millions of dollars per hour in industries such as retail or financial

services. This complexity often leads to critical mistakes such as inadvertently applying patches to a production database during business hours or giving an application developer or line-of-business user root-level access to a database, leading to system failure and downtime. In addition, when DBAs circumvent the standard change control processes to apply patches or modify code in these just-get-it-done situations, it creates a series of run-on operational problems in later build scripts, documentation, and baseline configurations that the IT organization relies on for vulnerability assessments. It is easy to forget that operational mistakes—actions not taken with malicious intent—are also risks that should be addressed with the appropriate IT controls.

23.4 HOW INTERNAL AUDITORS TEST DATABASE MANAGEMENT OPERATIONS

Most internal auditors have now been able to map policies to technical controls and have built cooperative relationships with corporate IT departments (and auditors within the IT department itself are becoming more commonplace). While the traditional tug-of-war between internal auditors and IT managers continues, there is a much greater understanding of the necessity for strong controls within IT departments. Many organizations are using IT controls frameworks such as CobiT, ITIL, or ISO to provide a foundation for these efforts and a common language to communicate between internal auditors and IT.

When it comes to auditing database operations, however, internal auditors have mistakenly left this issue as a minor risk that can be managed with a set of manual or compensating controls. The primary internal audit focus has often been on financial application/process-level controls, for example ensuring that the segregation-of-duties issues are enforced within an enterprise resource planning (ERP) application. Many financial compliance application/dashboard solutions do not include general IT controls at a granular enough level—exacerbating the application-centric focus for most internal auditors, who may forget to ask tough questions on who actually have access to view/modify/delete the data repository containing all the sensitive application data. As internal auditors get more sophisticated in auditing the complete end-to-end IT process, the issue of *data risk* is now moving to the forefront.

When internal auditors do take a close look at the critical database management processes, they typically find some of the following audit deficiencies:

- No clear segregation of duties for DBAs to avoid inappropriate data, schema, or audit log changes
- Lack of comprehensive reporting with a tamper-proof audit trail (auditing)
- Lack of capability to monitor who/what/when/where in the DBMS environment (auditing)
- Weak database security policies with too many highly privileged users (access)

- Lack of understanding or documentation of business data/private data (classification/encryption)
- Lack of security measures for data in motion and at rest (encryption)
- Lack of appropriate backup and recovery procedures (availability)
- Lack of security for database backups (encryption)
- Lack of strong application developer controls (access)
- Use by developer and Q/A procedures of sensitive production data for testing (encryption/masking)
- Lack of audited change management process (change management)
- Lack of vulnerability testing against baseline metrics
- Lack of resources and time for administrators to support the documented IT controls or process
- Poor awareness of appropriate IT controls within IT staff (training)

These typical deficiencies have resulted in a mix of manual or compensating controls that internal auditors have approved as adequate stop-gap measures to address the most serious risks. Internal auditors may operate under the misconception that databases are well protected and fortified within the company networks with built-in user security. Indeed, few internal auditors fully understand the typical risky behaviors of DBAs, such as stored procedures linking to external dynamic link library (DLL) files, passwords stored in batch files, and programs extracting private data into spreadsheets. In fact, inadequate manual controls on database processes may be the weakest link in the system of internal controls for most organizations.

Within some organizations, more than 50 percent of the IT controls are manual instead of automated controls. A sampling of these manual IT controls on DBMS environments that are currently in place within many organizations includes:

- Manual audit log file review at a certain time interval (samples)
- Manual review and tracking of user accounts to an approved request for setup and to ensure password aging is turned on
- Manuel sample review of change management system approvals
- Manual tracking of downtime since unauthorized downtime could be exploited by someone to manipulate the system
- Manual review of software patch management
- Manual review of the design of access control procedures
- Manual review of administrator and super user accounts and privileges
- Manual review of backup and disaster recovery plans to protect the data required for reporting

When companies are unable to implement a strong set of IT controls, they may need to document and implement a set of compensating controls in addition to the manual controls. In one scenario, the requirement may be to prevent

the DBA from inappropriately applying a patch on a production database during business hours to avoid any inadvertent system failure or data loss. The necessary combination of controls could combine a manual weekly review of the user access levels to certain production systems together with a change management process (submit-commit) for change requests to production systems with an audited approval work flow.

The value of manual IT controls such as spot-checking of application or database audit logs to detect suspicious user activity is highly dubious. Most DBAs would know to cover malicious activities by deleting or modifying their audit trail in the system logs, thus circumventing the ineffective manual control that the IT department labors weekly to enforce. Sometimes manual controls are linked and overlapping to create compensating controls—often creating a redundant and very costly web of ineffective controls.

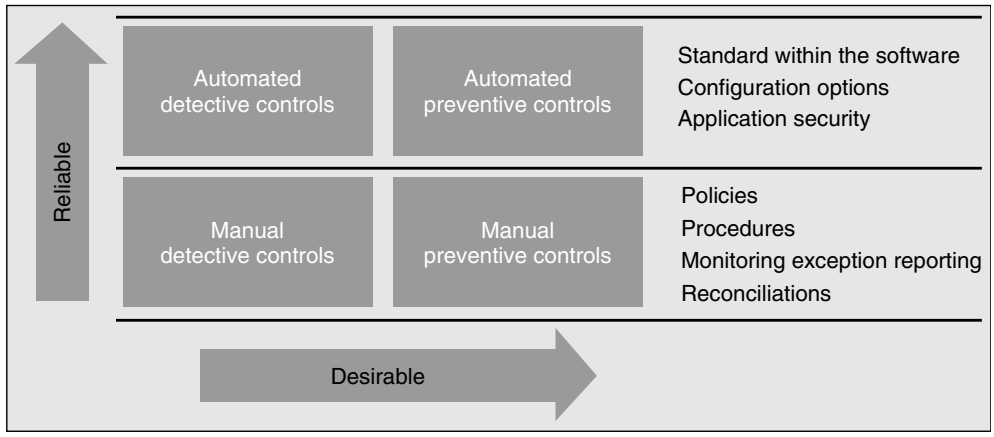
23.5 A FRAMEWORK FOR FORMULATING AN IT CONTROLS AUTOMATION STRATEGY

It is clear most IT organizations need a better framework to assess the effectiveness of IT controls and, in particular, to move toward a more automated set of detective and preventive controls for database management processes. Currently, most IT organizations are struggling under the cost of manual controls. In an October 2006 poll of 200 high-level finance and IT executives at public companies conducted by Fleishman-Hillard Research Group and Approva, more than a third (37 percent) said at least 40 percent of their IT controls still are manual, and 68 percent said at least 20 percent of their controls are manual.[10]

One effective way to assess controls effectiveness and understand how to improve IT controls automation is to use a simple framework such as the one created by Protiviti (Exhibit 23.2), a leading global risk advisory company. Protiviti distinguishes between detective controls, which help detect suspicious behaviors/patterns that indicate malfeasance, and preventive controls, which avert an activity from occurring altogether.

By segmenting controls into manual/automated and detective/preventive controls in a grid expressing the reliability and desirability of a certain type of control, the framework allows IT executives to develop an effective IT controls automation strategy. Evidently, not every enterprise database needs strong preventive controls with administrator segregation of duties and data encryption enabled. In many instances, it is adequate to implement an automated detective control by implementing a database auditing solution that may be much more cost-effective in the long run across hundreds of databases. This approach allows organizations to develop a cost-benefit framework that distinguishes between a nonessential Q/A database running inconsequential test loads and the HR production database containing all global employee personal identifiable information (PII).

The Protiviti framework also highlights the functional characteristics of an automated control. First, it does not require extensive software coding, third-party



Source: "Controls Intelligence: An Examination of How Robust Controls Analytics Can Improve Business Processes and Streamline Compliance," Protiviti White Paper, 2006. www.protiviti.com

EXHIBIT 23.2 HAVING MORE AUTOMATED AND PREVENTIVE CONTROLS PROVIDES A HIGHER LEVEL OF ASSURANCE

add-on security software packages, specialized reports, or manual reconciliations. Second, the most effective automated controls come standard within the RDBMS environment and require only configuration steps to implement. Finally, the automated control should support and enhance the application security without requiring any application code changes to run effectively (and make IT departments' lives easier in the process).

23.6 HOW TO IMPLEMENT EFFECTIVE PREVENTIVE CONTROLS FOR RDBMS

When measuring the effectiveness of data risk controls (RDBMS) in an organization, it is useful to evaluate the different preventive controls that are available to address the most frequent audit deficiencies. In theory, every database containing sensitive business data should be protected with strong preventive controls. In reality, however, many larger organizations have hundreds of databases from various vendors on different software versions scattered across many different data centers (and possibly different IT departments) and are at the outset unable to cover all databases at risk with strong preventive database controls due to the operational and financial impact. Instead, organizations should first complete a *data risk assessment* to determine what repositories to protect, where to implement strong automated preventive and detective controls, and how to tie these IT controls back to the overall organizational internal controls framework. The risk assessment should also include factors such as the technical feasibility of a certain

IT control. For example, encrypting all data in a database repository containing HR data seems like a sensible approach, until it becomes clear that the legacy HR application running on top of the repository does not actually support database encryption. In this case, a cost-benefit analysis would reveal that other effective automated preventive controls could easily replace data encryption at a much lower cost. (See Exhibit 23.3.)

When it comes to preventive RDBMS controls, the most common deficiencies found by internal auditors are in the areas of malicious/inadvertent data modification, administrator/super user access, lack of segregation of duties, and sensitive PII data encryption. These deficiencies pose such a high risk to any organization that prevention is paramount. Exhibit 23.4 highlights just how cumbersome it is to address these deficiencies using traditional manual preventive controls in the RDBMS environment.

Preventive controls also provide a set of operational benefits that can help justify the acquisition cost by themselves. For example, one of the most typical reasons (besides hardware failure) for downtime in production databases is simply human error. Too often there is a large number of DBAs and super users with root level access to production databases, and these users may inadvertently cause downtime by simple mistakes such as upgrading a script. An automated preventive database control offered by some RDBMS vendors implements flexible "security

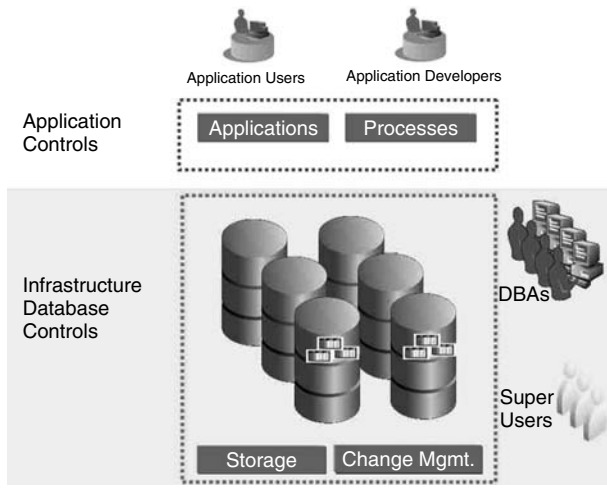


EXHIBIT 23.3 PREVENTIVE DATABASE CONTROLS ENSURE NO CHANGES CAN BE MADE TO PRODUCTION DATA, AND INTRODUCE SEGREGATION OF DUTIES FOR DBAS AND SUPER USERS

Objective	Manual Preventive (Example)	Automated Preventive
Avoid data change or modification	Manage database users manually at more fine-grained level and integrate with third-party change management systems	Use built-in DBMS capability or third-party software package
Lock down system "super users"	No effective manual control available (i.e., an organization would have to tag all data with individual security labels and rewrite all applications running on database)	Use built-in DBMS capability or third-party software package
Support application security and controls	Custom integration (including ongoing maintenance of integration points)	Use built-in DBMS capability or third-party software package
Avoid root-level access to database	No effective manual control available	Use built-in DBMS capability or third-party software package
Provide segregation of duties for DBAs and super users	No effective manual control available	Use built-in DBMS capability or third-party software package
Implement system of least privilege for new users	Manual process using separate manually maintained ACLs (database roles)	Use built-in DBMS capability or third-party software package
Masking test and backup data	No effective manual control available (i.e., tag all data with individual security labels and rewrite all applications running on database)	Use built-in DBMS capability or third-party software package
Avoiding inappropriate data-at-rest access	No effective manual control available	Use built-in DBMS capability or third-party software package
Avoiding inappropriate data-in-motion access	No effective manual control available	Use built-in DBMS capability or third-party software package

Exhibit 23.4 Comparing the Mechanisms of Manual and Automated Preventive RDBMS Controls

zones" within the actual database that cannot be accessed during business hours by administrators/super users, which can deliver dramatic cost savings and protect against external hackers at the same time.

At the end of the day, preventive database controls not only protect against evil insiders, but also provide an extra layer of security against external attacks, thereby enhancing the overall security stance of the organization.

23.7 HOW TO IMPLEMENT EFFECTIVE DETECTIVE CONTROLS FOR RDBMS

For the majority of data repositories in the average organization, it is simply not feasible to implement strong preventive controls in the short term. Instead, many organizations focus on effective detective controls that can alert internal auditors or security departments to inappropriate activity across many different repositories. Detective RDBMS controls primarily focus on data audit, system/configuration changes, and vulnerability testing.

A key aspect of data audit is to understand who accesses the RDBMS within a typical organization. Broadly defined, there are two types of connections to databases. (See Exhibit 23.5.) Automated connections consist of processes that will connect to the database at regular intervals (or will be triggered by certain processes) to extract or query the data. User connections are driven by an employee requiring access to complete a task or process. Both types of connections need to be covered when auditing database activity to ensure all potential data changes and access are captured.

While the multitude of connections in Exhibit 23.5 highlight the compelling flexibility and openness of the RDBMS environment, it also poses a challenge to more technically restrictive preventive controls such as data security labels or encryption. A poorly implemented preventive control could disrupt key IT processes when users or processes are suddenly denied access—a factor that increases the desirability of less-invasive detective controls such as database auditing to most overworked IT departments.

When it comes to data auditing, organizations today implement manual controls that negatively impact DBA and administrator productivity. Exhibit 23.6 underscores just how difficult—if not impossible—it is to address all the different facets of data auditing purely with manual controls.

Automated Connections	User Connections
Backup	Administrators
Reporting server	Application users
Replication	Casual users
Data integration	High-privileged users
Application integration	DBA super users
Data load/unload	Monitoring
Testing	
Extract, transform, load (ETL) data warehousing	

EXHIBIT 23.5 TYPES OF CONNECTIONS TO RDBMS THAT SHOULD BE COVERED BY DETECTIVE CONTROLS SUCH AS COMPREHENSIVE AUDITING (INCLUDING AUDIT EVENT CORRELATION/ANALYTICS)

Objective	Manual Detective (Example)	Automated Detective
Audit trail on DBA activity	Require each DBA to submit a daily e-mail summarizing all tasks involving access to production databases; includes reason for access and details of tasks performed while connected	Use built-in DBMS capability or third-party software package
Segregate access to audit event data	Assign written responsibilities to members of DBA team on specific personnel authorized to perform various database operations (start-up/shutdown, recovery operations, file reorganizations, etc.)	Use built-in DBMS capability or third-party software package
Protect audit trail	System administrator (super user) takes nightly image copy of database audit trail files	Use built-in DBMS capability or third-party software package
Audit trail on operating system (OS) log activity	System administrator (super user) takes nightly image copy of OS audit trail files	Use built-in DBMS capability or third-party software package
Detailed audit logging for changed data in database (before/after values)	Perform daily physical dump of journal files to ASCII and manually review contents	Use built-in DBMS capability or third-party software package
Ensure retention of audit history as per corporate security compliance regulations	System administrator ensures all image copy backups of audit trails are retained on system backup tapes for required time period	Use built-in DBMS capability or third-party software package
Ability to apply query analytics to historical audit data records	Reformat daily audit trail backup files, load into spreadsheet application or local PC database, perform summary analytics as needed	Use built-in DBMS capability or third-party software package
Provide accurate on-demand reporting of database and OS audit data	Write custom reports using audit data stored in spreadsheet application or PC database; manually retain the reports in a protected manner	Use built-in DBMS capability or third-party software package
Vulnerability testing	System administrator manually checks for common misconfigurations in the initialization parameters, profiles, user and role privileges, weak passwords, and so on, on every RDBMS instance	Use built-in DBMS capability or third-party software package

EXHIBIT 23.6 DETECTIVE CONTROLS FOR RDBMS CAN BE IMPLEMENTED USING MANUAL OR AUTOMATED METHODS

RDBMS vendors provide varying levels of data auditing capabilities built directly into their databases, providing baseline capabilities for anyone looking to audit a single database. Enterprise-wide database auditing, however, poses very different technical challenges, such as the computing processing overhead on production databases from fine-grained auditing and the requirement to centralize all audit data in a single place for reporting and analytics instead of storing the audit data with every individual database instance, scattered across the organization. In addition, data auditing is often missed in the initial IT project scope—from both a computing and a storage growth perspective—and the resulting lack of spare processing server cycles severely impacts DBAs' ability to implement data auditing at a later stage.

Internal auditors typically request many different kinds of broad audit reports from DBAs on an ongoing basis, and the resulting reports are rarely read and provide little value. Instead, internal auditors should insist that the audit trail is (1) *centralized*, (2) *segregated* from the DBA (who can otherwise modify log files to cover inappropriate activity), and (3) securely *retained*. Just as important are comprehensive reporting and analytics on the centralized audit event data with capabilities for issuing alerts or launching automated work flows when suspicious events are detected. For example, an automated alert could be generated if an administrator account is suddenly used to access HR payroll information outside normal business hours. A more advanced control in this case could go a step further and include an automated work flow for remediation that locks the suspicious administrator account until further investigation.

23.8 OUTSOURCED IT PROCESSES: THE PROMISE AND THE PITFALLS

Outsourcing, including offshoring business processes to emerging markets such as India or China, has been an important trend during the past decade and has created large-scale efficiencies for most organizations. To retain a competitive edge, most large enterprises are constantly evaluating what business or IT functions to outsource or offshore as part of their value chain. Outsourcing can allow an organization to refocus on core competencies instead of running extensive customer call centers or back-office processes such as payroll or data processing. Obviously, every decision to outsource a business process should include a careful risk assessment of the impact on IT security and the IT controls environment. Outsourced IT environments create a particularly challenging set of variables when implementing controls, and the inevitable loss of management control of IT processes includes a risk of disintegration of control standards between the company and the outsourcer.

According to Duke University and Ciber/Archstone Consulting, 49 percent of all offshore or outsourcing implementations are located in India, with up to 90 percent of worldwide outsourcing revenue going to India.[11] The success of India as a hub for outsourcing is good news for that country, but should also sound the alarm with internal auditors and corporate IT managers. In fact, the state of

IT security in India is bleak at best. In a 2006 survey, PricewaterhouseCoopers found that Indian companies lagged far behind the rest of the world in security practices.[12] The survey results reveal that Indian organizations score lower on every aspect of IT security compared with the rest of the world:

- Only 34 percent of Indian organizations have an overall security strategy.
- Only 26 percent conduct system penetration tests.
- Only 40 percent use encryption tools.
- Only 31 percent use intrusion detection tools.
- Only 29 percent use intrusion prevention tools.
- More than 29 percent have experienced financial losses from cybercrime compared with 19 percent for the rest of the world.

Without a doubt, Indian outsourcing companies have a better IT security stance than the average Indian organization, but taking a cautious tack when considering outsourcing to India makes a lot of sense. At a minimum, organizations should verify that the India-based outsourcer's security processes and policies are up to U.S. standards—and ensure a clear shared definition of the steps to fulfill a policy (e.g., what constitutes an employee background check). In one example, six employees of a BS-7799 and capability maturity model (CMM) level 5 certified call center in India were arrested in 2005 for swindling Citigroup customers out of $500,000 by convincing customers to share Social Security numbers and personal identification numbers (PINs) directly with the call center staff.[13] Organizations should never blindly trust a laundry list of security certifications from outsourcers, but instead implement aggressive processes to verify and test controls and security processes at regular intervals.

Another aspect to consider in an outsourcing arrangement is the motivation of outsourcing firms to actually report insider attacks. Since outsourcers have a desire to protect their revenue streams, they have a strong motivation to cover up insider abuse. They have little to lose unless the client finds out about the insider attack. Meanwhile, proactively reporting an insider attack could mean legal liability and damage to the outsourcer's reputation.

To boot, the insider threat in India is manifested in the extremely high turnover rates in outsourcing companies driven by an explosive growth in the sector. According to the consulting and research firm TPI, attrition levels have increased during the past two to three years, and currently the numbers quoted by various service providers range from 40 percent to an alarming 75 percent (annualized). The lower end of the scale would typically be associated with nonvoice (transaction processing) types of work, with the upper median representing voice-related work.[14] The constant personnel changes means new people are cycling in and out of the IT teams managing RDBMS environments, which in turn raises the risk of malfeasance from insiders.

This high risk of insider attacks suggests a company outsourcing IT processes to India should deploy more preventive RDBMS controls such as strong

segregation of duties for DBAs and controls to avoid inappropriate data access or modification. One way to control outsourced DBA processes is to ensure DBAs access databases only through a change management tool that provides built-in monitoring, user management, and auditing—and a single place to delete privileges when the employee jumps ship. And with the growing amount of data processing in India, organizations should also address end-of-life controls for data using encrypted backup mechanisms and data destruction policies.

The strong business case for outsourcing and offshoring certain business processes will continue to drive the outsourcing trend to countries like India and China. Many of the IT security concerns when outsourcing an IT or business process can be mitigated by including strong preventive and detective IT controls at the outset when the outsourcing process is designed. The proper inclusion of these controls can allow an organization to reap all the benefits of outsourcing without any of the potential catastrophic consequences of an IT controls breakdown.

23.9 THE COMPELLING BUSINESS CASE FOR AUTOMATED INFRASTRUCTURE CONTROLS

Most organizations leverage databases to run the most critical business processes, but have yet to implement strong and effective automated controls for database management. This oversight means most organizations may have left the back door open for insiders to commit abuse or fraud. Internal auditors have identified this risk and responded by requiring controls that have been typically implemented with a mix of manual and compensating controls that have become cost-prohibitive to maintain.

For IT departments looking to build a business case for RDBMS controls automation, it may be hard to initially quantify the benefit. Certainly, a circumstantial business case can be presented around RDBMS controls automation for the sake of mitigating risk and improving process visibility. It is hard, however, to quantify the return on investment (ROI) for risk avoidance, in case of an adverse event not happening. Another route to a quantifiable business case is to focus on the operational benefits and cost savings resulting from preventive or detective controls. Preventive database controls provide a long range of operational benefits, such as minimizing the high risk of inadvertent human error when DBAs and system administrators have to manage hundreds of business-critical databases. And preventive controls also allow organizations that have segmented data into many separate repositories to ensure separation of duties to consolidate these repositories into fewer central repositories with built-in fine-grained access rules by role. Detective database controls—such as a centralized auditing solution—help eliminate reporting redundancies and can streamline operations by providing direct insight into IT processes with real-time alerting when issues arise.

Controls automation is an imperative, and organizations should take the first steps today with automated preventive and detective IT controls. Given the

Standard Functionalities—Preventive Database Controls

- ☐ Protects the database and applications from unauthorized changes
- ☐ Restricts the DBA and other privileged users from accessing application data
- ☐ Enforces strong controls over who, when, and where application data can be accessed
- ☐ Enforces operational security policies
- ☐ Limits the use ad hoc query tools to bypass the application security
- ☐ Controls the use of powerful commands for DBA segregation of duties
- ☐ Supports IT/DBA outsourcing without compromising data security
- ☐ Supports online hosted applications without compromising data security
- ☐ Provides complete audit trail, reporting capabilities, and alerts
- ☐ No code change to existing application running on database
- ☐ Minimal impact on database performance and availability
- ☐ Encryption at rest and in motion

Standard Functionalities—Detective Database Controls

- ☐ Fine-grained database auditing
- ☐ Segregation of duties for audit data
- ☐ Safeguards audit data trail
- ☐ Audit event correlation across multiple systems
- ☐ Reporting and alerts with work flow hooks
- ☐ Support for heterogeneous database and application environments

Advanced Capabilities

- ☐ Audit event analytics packages
- ☐ Regulatory-specific reporting packages
- ☐ Integration with change management and work flow solutions

A special note of gratitude to the contributors to this paper: Kurt Lysy, Senior Solution Specialist (Oracle USA); Wynn White, Vice President, Security Product Marketing (Oracle USA); James Anthony, Business Development Architect, Global Sales Support (Oracle UK).

EXHIBIT 23.7 STANDARD FUNCTIONALITIES PREVENTION DATABASE CONTROLS

tangible business benefits, maybe it will turn out that smart companies can have their cake and eat it, too—at least when it comes to simplifying IT controls.

When selecting security and IT controls automation solutions for an organization's database infrastructure, Exhibit 23.7 contains critical capabilities as discussed in this chapter.

Notes

1. Vivien Tero, "Worldwide Compliance Infrastructure Forecast 2006–2010," IDC, 2005, www.idc.com. IDC defines compliance infrastructure as spending on "the enabling technologies and services that allow companies to control four primary areas: information integrity, process integrity, controlled access, and information retention."

2. French Caldwell et al., "Survey on Sarbanes-Oxley Compliance Practices within IT Organizations and Businesses," 2006, www.gartner.com.
3. "The Global State of Information Security 2006," PricewaterhouseCoopers, www.cio.com.
4. Charles J. Kolodgy and Christian A. Christiansen, "Using Security Compliance Software to Improve Business Efficiency and Reduce Costs," IDC White Paper, 2005, www.idc.com.
5. Joe Drape, "Horse Racing: Pick-Six Fix Admitted as Giuliani Steps In," *New York Times*, November 21, 2002, www.nyt.com.
6. Noel Yuhanna, "Database Security and Auditing as a Compliance Solution," Forrester Research, February 2006, www.forrester.com.
7. Fred Cohen, "Defending Against the Evil Insider," Burton Group, November 16, 2006.
8. Noel Yuhanna, "Enterprise Databases Need Greater Focus to Meet Regulatory Compliance Requirements," Forrester Research, January 2007, www.forrester.com.
9. Wikipedia, "Database Administrator," http://en.wikipedia.org/w/index.php?title=Database_administrator&oldid=101767664_.
10. Melissa Aguilar, "Experts Expect Surge in IT-Controls Automation," *Compliance Week*, October 17, 2006, www.complianceweek.com.
11. "Second Bi-annual Offshore Survey Results," Duke University and Ciber/Archstone Consulting, December 2005, https://offshoring.fuqua.duke.edu/pdfs/2nd_highlights.pdf.
12. See note 3.
13. Saritha Rai, "Indian Outsourcers Move to Fix Security," *International Herald Tribune*, June 17, 2005, www.iht.com/articles/2005/06/16/business/security.php.
14. Dinesh Goel and Prabhash Thakur, "India: An Attractive BPO Destination Marred by Alarming Attrition—Insights into the Causes, Impact and Mitigation Actions," TPI, www.tpi.net/knowledgecenter/whitepapers/.

CHAPTER 24

PLM TECHNOLOGIES: ROLE AND VALUE IN SUPPORTING PRODUCT COMPLIANCE

Richard Kubin

24.1 INTRODUCTION

Product compliance requirements have always been a factor in the design, manufacture, and sale of goods and services worldwide. Many of these are regulated by government agencies, such as those administered in the United States by the Federal Communications Commission (FCC), Food and Drug Administration (FDA), and Federal Aviation Administration (FAA), and are primarily aimed at protecting the public safety. There are also requirements to comply with other product- or policy-level criteria, which may be defined and controlled by the producing company. These may include quality and reliability, but may also include more esoteric requirements, such as the labor practices of companies supplying materials or manufacturing services. Recent regulations, like the European Union's Restriction of Hazardous Substances (RoHS)[1] in electronic products, have had a large impact across the affected industries and their entire supply chains and have raised the visibility of both the requirements and the difficulties in meeting them.

The outsourcing and globalization of manufacturing add further complexity to product-level compliance, particularly in the electronics segment. A product may be designed in the United States, its components sourced from hundreds of suppliers across multiple countries, assembled by a contract manufacturer in China, and shipped to Europe for distribution and sale. To ensure that none of

the components or materials used in the finished product contain any of the six banned RoHS substances above allowable thresholds is a difficult task—to be able to provide documentation of this compliance that extends down through the supply chain is even harder.

While such compliance management may be possible using manual, paper-based processes, the shortened product life cycles and competitive pressures common in many industries require a more systematic approach. The definition and development of software to support product life cycle management (PLM) processes provides a basis for product compliance management. Technology that extends these processes across the entire design and supply chain, along with the development of supporting data-exchange standards, now allows companies to automate and control much of the activity and information required to ensure compliance.

24.2 PLM—WHAT IT IS, AND WHAT IT ISN'T

Product life cycle management (PLM) is a complex, misunderstood, and perhaps misrepresented field, and there is little agreement even to a standard definition. The following provides a general definition: PLM is a strategic business methodology that delivers tactical capabilities for new product development, delivery, and support, from ideation to end of life. This is accomplished through solutions that collaboratively manage the product life cycle across the extended enterprise. These solutions are built upon underlying business and engineering processes, which are then combined with supporting software technologies and network infrastructure. These processes span the multiple tiers of today's extended value chains, for design, manufacturing, delivery, and service/support. By extension, this requires the exchange of data between multiple disparate systems, across multiple enterprises.

From this general definition it can be interpreted that PLM is not a single software system that can be installed and operated within the four walls of a company; it is a set of processes that are supported by a loosely connected framework of applications, databases (information), and people.

Some experts have provided a definition in terms of PLM functionality, such as:[2]

- Product data management (PDM) (20%)
- Product and process definition (15%)
- Configuration management (10%)
- Collaboration software (10%)
- Customer-oriented applications (10%)
- Supplier-oriented applications (5%)
- Integration (5%)
- Data exchange (5%)
- Visualization/viewing (5%)

- Definition and management of product life cycle processes (5%)
- Project management (5%)
- Portfolio management (5%)

In this case, the percentage values are meant to represent the relative contribution to a complete system, and are an example only. While PDM plays a key role, there are clearly many other elements required to provide a complete solution that spans the entire virtual enterprise. Product compliance management can be viewed as an integral subset of PLM functionality.

24.3 THE PRODUCT

Product life cycle management takes an approach that is very product-centric—nothing exists within the system without being directly related to a product in some way. The product is generally defined by a set of documentation, typically including: product specifications that define the physical and performance attributes; a bill of materials (BOM) that defines the specific components, materials, and quantities required to manufacture the product; and a set of engineering files (schematics, Engineering Computer Assisted Drawing (ECAD) and Manufacturing Computer Assisted Drawing (MCAD) that specifically define the electrical and mechanical attributes). Where a company controls the BOM, it also typically controls the approved manufacturer list (AML) and/or the approved vendor list (AVL) for each of the BOM items. In cases where the branding producer is using an original design manufacturer (ODM), it may define and maintain only the product specification, and the ODM is responsible for the detailed design, BOM, and AVL/AML.

In general terms, product compliance starts with the physical and functional design and the BOM and AVL/AML, but also extends to the manufacturing processes used to assemble the finished product. The specific compliance requirements then dictate what processes, information, and in some cases validation, are required based on the product and its target market.

24.4 THE REQUIREMENTS

As previously mentioned, compliance requirements come from many places, but are generally based on regulatory jurisdictions and product category. For example, an automobile designed and built in Germany that is to be marketed in the United States must meet the safety requirements of the National Highway Traffic Safety Administration, including provision of sample vehicles for crash testing, as well as emissions requirements, which may vary by state.

In the case of regulatory compliance requirements, proof of compliance is also largely dependent on the specific regulation, enforcement approach, and potential for harm to people or the environment. In many cases, testing by independent accredited laboratories is required, with the test reports submitted to the regulatory body. In other cases, such as with the European Union's RoHS

directive, the fact that an electronic product is available for sale in an EU country is a self-declaration by the producer or importer that the product complies with the RoHS directive. If there is any doubt from the EU country's regulatory authority, they can request technical documentation from the producer that supports RoHS compliance, or they may perform analytical testing themselves.

Compliance requirements also go beyond those imposed by regulatory bodies. From a product design perspective, components and materials selected from external sources for use in the product must meet certain physical and performance criteria, which are generally defined in a procurement specification or defined in the associated engineering files (ECAD/MCAD). Manufacturing processes may also be stipulated within a specification. Supplier compliance to these specifications is often the largest contributing factor to the manufacturing yield and quality of the product, where quality refers to the reliability of the product as well as to whether it performs to its specification. In many cases, supplier noncompliance to the component specifications not only may impact manufacturing yield, but also may lead to product noncompliance of regulatory requirements. In this manner, compliance could be considered an integral element of quality processes, but one that may have far-reaching consequences. The recall in 2006 of an estimated 10 million laptop batteries manufactured by Sony[3] for possible overheating also affected Apple, Dell, Fujitsu, Lenovo, and Toshiba, which were using Sony as a battery supplier.

The common thread is the linkage to the product record, with clear association of BOM, AVL/AML, component/material specifications, and supplier compliance information. However, this thread does not end with the release of the product to manufacturing.

24.5 THE PROCESSES

Compliance requires scrutiny and diligence across the entire product life cycle. Primary compliance activities must take place during design, taking into account the target market and applicable regulatory requirements. However, compliance diligence must continue throughout the manufacturing of the product, during any repair or refurbishment, and also through to the end-of-life stage. In many cases, there are specific requirements for supporting the take-back and recycling of products once their useful life is complete.

Viewing compliance as an integral part of overall quality processes naturally leads to reference of the ISO 9001 standards.[4] The primary focus of ISO 9001 is to define clear expectations around quality management practices, processes, and documentation. Process control, monitoring, and demonstrated adherence to the processes are key. While it is possible to be ISO 9001 compliant using manual paper-based processes, this is neither practical nor cost effective for most companies. Software technologies exist to support process definition and execution of associated work flows, while also maintaining the process state and all interaction history. Further, new technologies and data-exchange infrastructure to

extend these processes across a multitier supply chain are changing the compliance landscape. In industries such as electronics, where product life cycles are short and competition is strong, advantages can be obtained by integrating these collaborative elements within the overall PLM infrastructure.

24.6 COMPLIANCE ASSURANCE SYSTEM

In May 2006, the European Union's RoHS regulators released a document titled "RoHS Enforcement Guidance Document."[5] This was based to a large extent on work done by the United Kingdom's Department of Trade and Industry in researching practical means both for manufacturers to comply with RoHS and for regulatory bodies to enforce it. While there are still many uncertainties relating to RoHS enforcement, the guidance document outlines some expectations on how companies could manage and document their compliance processes. The document suggests that larger companies would be well advised to implement a compliance assurance system (CAS), which would provide formally defined processes and is integrated within the organization's quality and management systems to cover compliance both within the company and within the supply chain. The system would include a technical documentation system to support the compliance process, assure validation of conformity to requirements, and provide necessary tools and infrastructure to support the exchange and management of supporting data, including material declarations and supporting documentation. Further, evidence is required that the system is being followed, including results of product-specific conformance assessments (including justification of RoHS categorization and use of exemptions), availability of materials declarations and substance analysis, as well as evidence of procurement, inventory, and production controls.

Building on these recommendations and providing a more practical description, a CAS can be defined as an integral subset of an overall PLM system that provides:

- Compliance process definition
- Compliance rule definition
- Managed execution of work flows across the supply chain
- Process state management and visibility
- Managed collection of compliance data from suppliers
- Support for data-exchange standards
- Association of compliance data with components, suppliers, and products
- Automated analysis of data against compliance rules
- Alert generation
- Closed-loop corrective action process management
- Closed-loop preventive action process management

Such a system should provide the capability and flexibility to support multiple aspects of product compliance. It should support the process execution and

collaboration with trading partners and ensure direct association of compliance data with the parts and suppliers of record. Secure retention of all data, including an auditable record of all user and system interactions, is also a key requirement.

24.7 VALUE OF AUTOMATION AND SYSTEM CONTROL

By applying available technologies for multicompany business process management, systems integration, and automated business-to-business (B2B) data exchange, a compliance assurance system can provide business value in a number of areas. The most obvious is the reduction of manual effort required to manage the processes, such as requesting and collecting supplier compliance data, data entry, compliance analysis, and report generation. Directly associated with the reduction of manual processes through automation and B2B data exchange with suppliers is the improvement in data quality—having fewer errors means less time spent on validation and correction, as well as reduced risk.

While the implementation of such a system may be justified based on the direct cost savings alone, other benefits have the potential to far outweigh these. These can be grouped into two categories: risk mitigation and extension of the base collaboration system to support additional compliance needs or business processes.

The risk events or drivers and the potential impacts will vary across industries and the regulatory frameworks that govern them, as will risk mitigation strategies. The ability to proactively manage compliance and identify potential issues early (preferably before they can impact end users or customers) can provide very high value in many cases. Without knowing the details and root cause(s) of the Sony laptop battery recall, one could hypothesize that if there was an opportunity to identify the problems before 10 million potentially defective batteries were shipped, the value would be tremendous.

Proactive risk management analysis techniques are available[6] that define risk models to evaluate different mitigation strategies. These models can be very effective in helping to identify the specific risk elements and potential for solutions to modify the impacts, and therefore provide an objective valuation of possible cost avoidance that can be a large factor in supporting the business case for implementation of a compliance assurance system.

The third area of benefit is in leveraging the CAS and its integration with PDM and other internal systems, along with the improved supplier communication channels, beyond the initial scope. This requires companies to take a more holistic view of product compliance and to explore other opportunities for business process improvement that may be supported by the same trading partner communication platform. This must generally be done from the strategic executive level, rather than the tactical component engineering or procurement level.

A good example can be found in how various electronics companies reacted to the EU's RoHS directive challenges. Many saw this primarily as a lead-free initiative and made the assumption that the supply chain would change on its

own and therefore proactive compliance processes, and systems to support them, were unnecessary. The electronics industry is now faced with a number of additional environmentally related regulations, including "China RoHS" (which is different from the EU version), REACH (EU regulations on use of chemicals), and the EU's Design for Energy Using Products. These all add additional compliance requirements that are all related to the product. A compliance assurance system should have the flexibility to extend to support additional compliance attributes—these can also include compliance to technical and quality specifications.

24.8 REFERENCE ARCHITECTURE

A number of leading electronics companies, including component/subassembly providers, electronic manufacturing service providers, and original equipment manufacturers (OEMs), are deploying or designing a compliance assurance system that will support the controlled collection and management of material declarations and supporting documentation using emerging XML-based data-exchange standards. Standards-based declarations and reporting will reduce both the internal costs and the costs borne by suppliers and manufacturers. Supplier on-boarding using standard formats will be faster and smoother, as they will be able to establish a library of declarations and reuse these across multiple customers.

In order to support the previously defined criteria for a compliance assurance system and automate and control associated processes, the following solution requirements are defined:

- Support for process definition, execution, and monitoring, across internal and external entities
- Support for automated request generation and collection of compliance documents from suppliers, including support for data exchange standards where available
- Support for both system-to-system data exchange and human interface to ensure access for all suppliers
- Establishment of a clear audit trail for all related supplier transactions to support supplier accountability for the documentation that is provided
- The ability to ascertain the compliance of parts and suppliers to the applicable regulatory compliance requirements
- The ability to ascertain the compliance of parts and suppliers to internal or customer-specific compliance criteria
- Product-level compliance analysis and reports by associating item-level information with a product bill of materials
- A controlled process and data record to establish proof of regulatory compliance due diligence
- A means to define, identify, and track any allowed exemptions that may be exercised, both at the component/item level and at the product level

- Support for the request and collection of additional electronic documents to support compliance, such as third-party laboratory reports, and associate this data with the respective items
- Support for closed-loop supplier corrective/preventive action processes

An effective compliance assurance system can be established within the framework of PLM and can leverage existing systems such as PDM and enterprise resource planning (ERP). XML-based structures for declarations and other standard document types can simplify data exchange. Available technology to support data management, analysis, and intercompany processes and data exchange, coupled with the methodologies and practices of ISO 9001 for quality process and documentation management, complete the picture. Such a system provides the required support for compliance and process control, thereby mitigating the risk and ensuring supplier accountability while reducing the overall costs through automation and higher data quality.

Exhibit 24.1 provides a view of a reference architecture for such a compliance assurance system. The primary elements are:

- *Compliance database:* provides a secure repository and relational database to connect supplier compliance data with items and product structures
- *Corrective action request management:* provides a closed-loop system with defined work flows, automated notifications, escalations, and approvals; supports capture and documentation of noncompliance cost impacts to support supplier charge-back

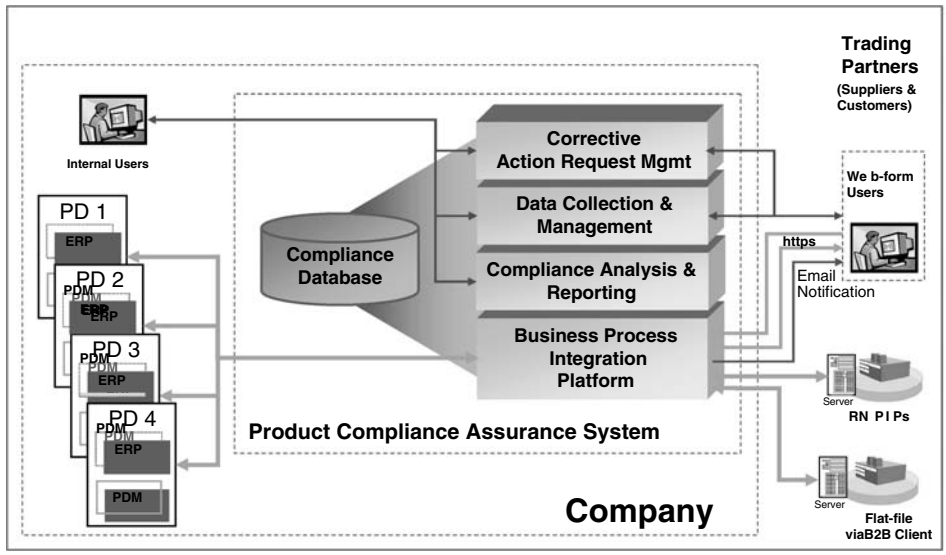


EXHIBIT 24.1 REFERENCE ARCHITECTURE FOR A COMPLIANCE ASSURANCE SYSTEM

- *Data collection, approval, and management:* provides automation and control of processes to collect compliance data from suppliers, with support for data standards where available; approval routing where necessary; full audit trail of all interaction and submissions.
- *Compliance analysis, alerts, and reporting:* provides analysis of supplier compliance data and supporting documentation against required compliance criteria; automated alert generation for noncompliant situations; generation of item-level and product-level compliance reports.
- *Business process integration platform:* provides integration with internal systems, including capability to support multiple divisions or business units that may be operating distinct PDM or ERP systems; provides technology to support automated data exchange and validation between trading partners; supports mapping and automated transforms to normalize and validate data.

24.9 CONCLUSIONS

Product-level compliance has become a very complex exercise for many companies and industries. Regulatory compliance in some industry sectors, such as aviation and pharmaceuticals, is reasonably well understood and has been entrenched in the new product development and production processes. Other sectors, such as consumer electronics, have in the past been primarily focused on safety and electromagnetic emissions, which are essentially design elements, and have not significantly involved the supply chain. Newly implemented regulations, such as EU RoHS in 2006 and REACH in 2007, have much broader impacts that clearly extend across the entire supply chain.

The principles of quality process management defined under ISO 9001 are well suited to the management of product compliance. The definition and deployment of a compliance assurance system within the framework of product life cycle management that builds on the ISO 9001 processes and extends these across the supply chain is changing the way that many companies are managing compliance. The availability of software designed to manage intercompany processes now allows companies to integrate key internal systems such as PDM and ERP with controlled collection of supplier information and compliance analysis to better manage the growing risks associated with noncompliance.

By taking a more holistic view of product compliance management that includes supplier quality attributes as well as regulatory requirements, such a system can provide significant benefits in the proactive monitoring of supplier compliance against multiple criteria. This allows better visibility to identify noncomplaint situations within manufacturing operations before they can impact the market and end user. The overall cost to support these activities can be reduced through the use of automation and standards-based system-to-system integration and data exchange.

Notes

1. Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, *Official Journal L 037*, February 13, 2003, 19–23.
2. John Stark, *Product Lifecycle Management—21st Century Paradigm for Product Realisation* (London: Springer-Verlag, 2005).
3. "The Fallout from Sony's Battery Recall," *USA Today*, October 2, 2006.
4. ISO 9001, International Organization for Standardization, Geneva, Switzerland.
5. EU RoHS Enforcement Authorities Informal Network, "RoHS Enforcement Guidance Document," May 2006, www.rohs.gov.uk/Docs/Links/RoHS%20Enforcement%20Guidance%20Document%20-%20v.1%20May%202006.pdf.
6. Preston Smith and Guy Merritt, *Proactive Risk Management* (New York: Productivity Press, 2002).

CHAPTER 25

HOW XBRL WILL DRAMATICALLY IMPROVE REPORTING AND CONTROL PROCESSES

Robert G. Eccles
Liv Watson
Mike Willis

25.1 INTRODUCTION

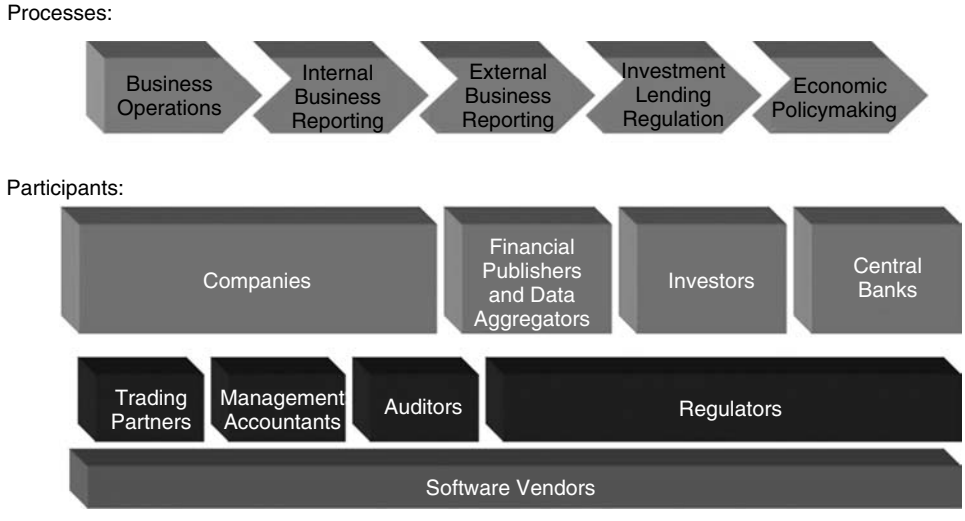
Investors who risk their hard-earned cash in equities need access to timely, relevant, and accurate financial and business information. Most of this information originates with the companies whose stocks they own. For the capital markets to operate most efficiently, information about public companies must be understandable, accessible, accurate, and, most important, trusted by market participants. In the current state of information access, there are multiple problems in making this level of clarity, accuracy, and public trust a reality.

One of the biggest roadblocks is that this information is provided in many different proprietary data formats, making it difficult to access, integrate, and analyze in a timely, complete, and accurate manner. The Internet and electronic communication have ensured that information is more freely available than ever before and that the time it takes to deliver that information has sharply decreased.

The key question now is: How reusable is that information? Even when you know exactly what you are looking for and roughly where to find it, extracting information from financial and business reports today generally involves a frustrating experience and a time-consuming and largely manual effort. The biggest problem is that the format and media in which financial and business reporting data are presented vary widely among paper, Hypertext Markup Language (HTML), Portable Document Format (PDF), and other human readable forms or proprietary electronic formats tied to a specific software application. Each publishing format has its limitations, and they can all be interpreted only by manual human processing.

To resolve the problem of providing reusable access to timely, relevant, and accurate financial and business reporting information on demand, a market-driven open-standard consortium has been organized to develop an information standard called eXtensible Business Reporting Language (XBRL).[1] This consortium powerfully connects members representing the entire financial and business reporting supply chain (see Exhibit 25.1) in the development of a standards-based solution for financial and business reporting information that is universally open, industry driven, and internationally endorsed. In simple terms, XBRL is a technical supply chain standard for moving financial and business reporting information into an interactive intelligent information format.

The worldwide development of XBRL is governed by XBRL International, a not-for-profit collaborative consortium comprised of over 600 organizations (including companies, institutional investors, and government agencies) from 27



Source: XBRL International.

EXHIBIT 25.1 THE FINANCIAL AND BUSINESS REPORTING SUPPLY CHAIN

countries. The consortium is organized into national jurisdictions and operates via electronic collaboration tools, conferences, and meetings. Members of the consortium are committed to collaborate in the development of the XBRL information standard, to promote and support its adoption, and to incorporate the consortium's work into their products and services.

25.2 A PRIMER ON XBRL

There are two main components to XBRL: the XBRL Specification and the XBRL Taxonomies, including the underlying linkbases.

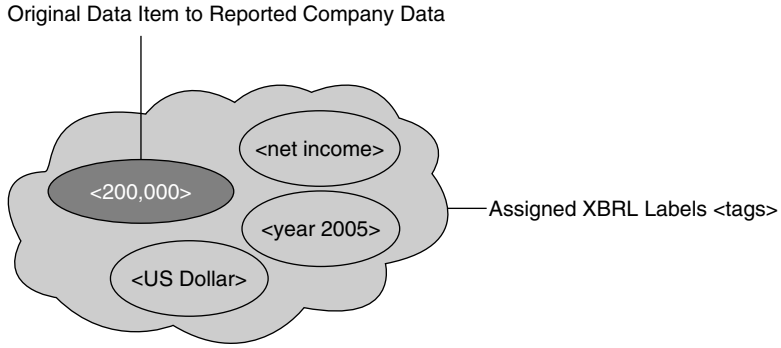
(a) XBRL SPECIFICATION. The Specification provides the fundamental technical definition of how XBRL actually works. The documentation of the Specification is published by XBRL International and is available at www.xbrl.org/specifications/. The XBRL Specification was developed from the beginning to satisfy three distinct kinds of requirements:

1. Business requirements
2. Technology requirements
3. Political requirements

The documentation of the XBRL Specification is the primary building block for ensuring that XBRL exists as a nonproprietary and interoperable information format. The XBRL Specification documentation sets out the technical guidelines for XBRL and is aimed primarily at software professionals who are seeking to build tools that will directly create or consume XBRL documents.

(b) XBRL TAXONOMIES. The key to understanding the benefits of XBRL lies in the notion of taxonomies, and it is probably time for all executives to add "XBRL taxonomies" to their professional vocabularies. The word *taxonomy* is derived from the Greek words *taxis*, meaning arrangement or division, and *nomos*, meaning law. XBRL taxonomies are basically dictionaries of business terms and their corresponding tags. The result of separating content from presentation is what Securities and Exchange Commission (SEC) chairman Christopher Cox likes to call "interactive data." Once information is made interactive, it is much easier to reuse. Not only is the information instantly searchable and retrievable, but it can also be immediately loaded into spreadsheets and any number of software applications for analysis. Exhibit 25.2 shows a sample of an original data item with explanatory labels that enhance the user's understanding of a data element.

The enormous advantage of universally accepted taxonomies is that they allow for a systematic way of naming and organizing financial and business information into groups that share similar characteristics, thereby enriching the user experience and streamlining the preparation processes. The idea behind this is simple. Instead of treating information as a block of text, an XBRL taxonomy provides an identifying tag for each individual item. These tags are standardized regardless of company, industry, country, or accounting regulation. Business



Here, the basic data point, <200,000>, is enriched by XBRL tags that fully explain the context of the number. It is net income from the year 2005 and it is reported in U.S. dollars. The labels form a relevant context or structure (such as a particular chart of accounts). Tagged data can be extracted for use in other reports, analytical software, and databases and still maintain its original, meaningful context. The labels are standardized regardless of company, industry, country, or accounting regulations.

EXHIBIT 25.2 STANDARDIZED LABELS IDENTIFY THE MEANING OF EVERY NUMBER

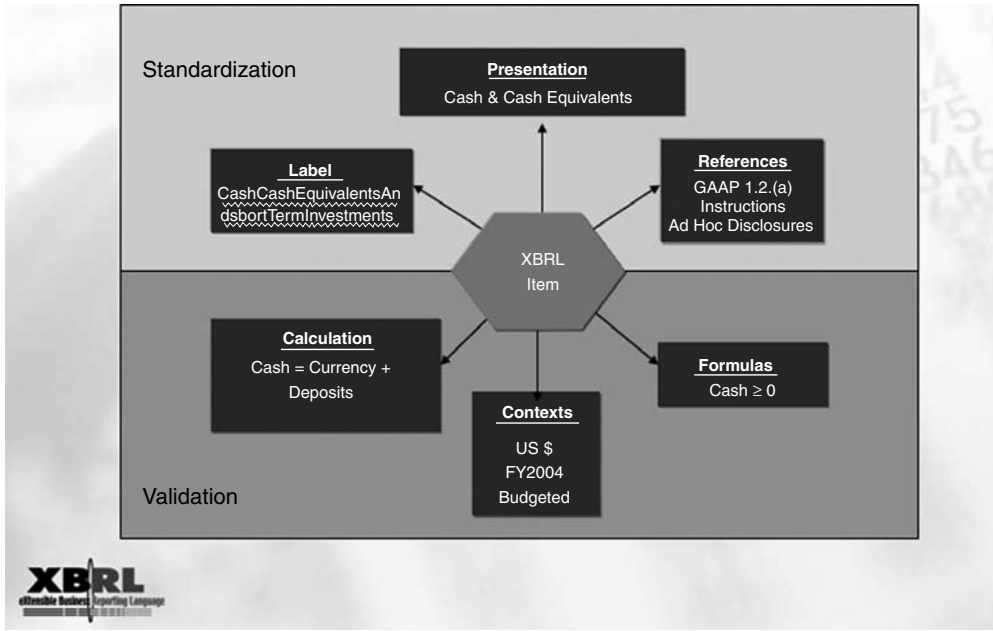
information reported in XBRL can be easily extracted for reuse in other reports, analytical software, and databases and retain its original, meaningful context.

In XBRL information is both humanly and machine readable. In the example in Exhibit 25.2, the basic data point, <200,000>, is enriched by XBRL tags that fully explain the context of the number: <200,000> is net income from the year 2005 and it is reported in U.S. dollars. These lists of specific labels—as developed by the consortium of market participants—are the XBRL Taxonomy Framework and can be extended (i.e., modified) by individual companies to customize the "business dictionary of definitions" to reflect their unique reporting needs.

One of the greatest benefits of XBRL is that it allows for additional attributes to travel with a data item throughout its life cycle. XBRL refers to these additional attributes as "linkbases." These linkbases are similar to hyperlinks on the Internet, except that rather than being physical point-to-point linkages, they provide a reusable contextual relationship between concepts that can be applied to the elements regardless of where they physically reside. Currently the XBRL Specification allows for six different types of linkbases as outlined in Exhibit 25.3.

25.3 WHO IS USING XBRL TODAY?

Today the use of XBRL is primarily being driven by regulators and government agencies around the world. For example, every Chinese public company is required to report its financial statements in XBRL to the Shanghai and Shenzhen



1. **Label.** This is a list of common accounting terms that is used in general purpose financial statements.
2. **Presentation.** This allows the user to click on a link and see the information in different views, such as different languages.
3. **References.** This allows for data items to be linked directly to items in authoritative literature such as U.S. GAAP standards.
4. **Formulas.** This allows one to set triggers that could give early warning signals for accounts that are in trouble with one click of the mouse.
5. **Contexts.** This gives the XBRL tagged item more information about the data item, such as it is a budget number in U.S. dollars for fiscal year 2004.
6. **Calculation.** This explains from what calculation the number derives, for example ensuring the cash equals currency plus deposits.

Source: XBRL International.

EXHIBIT 25.3 XBRL LINKBASES

stock exchanges. XBRL projects also exist in Belgium, Denmark, Dubai, India, Japan, Spain, Sweden, the United Kingdom, and the United States, to name a few locations. This raises the question: "Can any capital market afford to not bring dynamic, interactive, and intelligent financial and business information to the marketplace?" Those markets that increase transparency through XBRL will benefit from greater liquidity and a lower cost of capital. Those that do not will be losers in the global competition for capital.

One of the most publicized initiatives regarding XBRL is the U.S. SEC's announcement of a $50 million contract to upgrade its EDGAR electronic filing system for XBRL compatibility. The SEC has provided an additional grant of $5.5

million to XBRL U.S., Inc. to complete the U.S. generally accepted accounting principles (GAAP) XBRL Taxonomy. To signal the importance of this initiative, SEC Chairman Cox has been promoting the benefits of XBRL in public speeches and in testimony before Congress.

Here are some other noteworthy initiatives regarding XBRL:

- *U.S. Securities and Exchange Commission.* At an open Commission meeting on January 31, 2007, the Commission voted unanimously to issue a proposed rule for allowing mutual funds to report the risk/return portion of a mutual fund prospectus under the voluntary XBRL program.
- *Federal Financial Institutions Examination Council (FFIEC).*[2] In October 2005, U.S. banking regulators mandated that all U.S. banks must file their periodic call reports in XBRL as part of a dramatic regulatory process improvement effort. The result was a reduction in the time to analyze the call reports from 45 days to two days, dramatic reduction in error rates from 68 percent to under 5 percent, and significant automation of previously mundane and highly manual process steps, resulting in the redeployment of approximately 800 employees.
- *The Netherlands.*[3] In 2005, the Dutch government began an XBRL-enabled compliance process reengineering effort driven by the collaboration of all Ministry of Finance and Ministry of Justice agencies. The stated goal of the project is to reduce the compliance burden on companies by 25 percent. This program was implemented on January 1, 2007, and provides Dutch companies with the ability to significantly streamline all of their government-related compliance filings.
- *Banco de Espana.*[4] The central bank of Spain implemented XBRL-enabled compliance processes in 2005 and expanded its program in 2006 to cover more of the required filings. This high-profile central bank has played a leading role in the development of the Basel II XBRL Taxonomies now being implemented across central banks of EU countries.

Perhaps one of the most important global initiatives over the next few years regarding XBRL is in Europe. It could potentially affect over 50 million European companies. At the second XBRL Conference of the European Companies Register Forum hosted by Bolagsverket (Swedish Companies House) in January 2007, several European regulatory agencies committed to mandatory use of XBRL in their national filing process in the next few years. The European Companies Register Forum is made up of Companies Register Authorities ("Companies House") from all European countries and other Commonwealth countries as well, such as Australia, Hong Kong, and Singapore.

The purpose of the one-and-a-half-day meeting was to provide a status update on what is going on in the different member countries. Several of the speakers confirmed they plan to go for a mandatory use of XBRL in their national

filing processes. For example, a speech by a representative of Ireland's Department of Enterprise, Trade, and Employment[5] stated that it is working together with the Companies Register Office (CRO),[6] and they are committed to making XBRL be used by every single Irish company. From the UK, Ross James from Companies House confirmed its commitment to XBRL as the best solution for it to face its challenges: 2.3 million new limited companies in 2006 (a rate of 120 new ones every hour) with 40 documents being filed every second. Bolagsverket itself confirmed that it has been receiving e-filings in XBRL[7] since July 1, 2006, and that it plans on making XBRL mandatory.

These initiatives show that market adoption of XBRL is accelerating around the world. The XBRL Consortium provides periodic updates on market activities,[8] and there is a Wikipedia[9] site available for collaborating on current market efforts. These efforts, taken together, will result in the use of XBRL in some fashion by over 50 million companies at the end of 2007.

25.4 THE BUSINESS CASE FOR IMPROVING BUSINESS REPORTING TRANSPARENCY

The accelerating adoption rate of XBRL within the regulatory community has had some very positive benefits, such as the building of taxonomies, increased training, and the development of software. However, the fact that most of the application of XBRL has been in the regulatory realm has also created some skepticism and concern by companies. Management teams commonly view XBRL as a technology that has to be implemented when mandated by regulatory agencies. As a result, many are taking a wait-and-see approach to internal adoption and implementation.

This approach is reasonable; however, it reflects a narrow view of XBRL and the process enhancements this information standard makes available. The pervasive problems within the business reporting supply chain do not exist only at the reporting and regulatory end of the supply chain. They exist within the companies themselves and between companies and their trading partners. When assessing adoption of XBRL and other supply chain standards, management teams should consider the typical economic consequences of standardization:

- Lower costs
- Improved accuracy
- Higher volumes of information available for analysis
- Accelerated frequencies of availability
- Improved resource allocation
- More efficient processes

25.5 CURRENT CONSTRAINTS

Before discussing the process enhancements enabled by XBRL, it is useful to clearly understand the pervasive problems that XBRL is specifically designed to

address. What follows is a list of some of the primary constraints on reporting and compliance processes as they exist today:

- *Proprietary software formats inhibit reuse.* Business information contained within a proprietary software format (e.g., .doc, .pdf, .xls, etc.) is not reusable by other proprietary software applications in a cost-effective manner. The information can be exported to another application, but in this transfer process virtually all contextual information relevant to processing the information is lost. This simple problem results in manual, costly, slow, time-consuming, and complex compliance and analytical processes as data are transferred from one application to another. In addition, the related compliance controls and completeness assessments are also often manual.
- *Business information concepts are application specific.* Many companies have "standard general ledger" and/or "corporate entity" concepts; however, these internal accounting and reporting standards are typically applied within a single software application, global data warehouse, or other proprietary application. Although these concepts are valid across the full range of company-wide disparate software applications, the proprietary nature of these applications makes it impossible to share data and analysis across them. Systems integration is only a partial solution and does not provide a cost-effective, adaptable, and sustainable solution. The pervasive problem here is the need for information to carry with it across disparate applications its full contextual structure.
- *Analytical formulas are physically defined.* Analytical formulas embedded in spreadsheet and other proprietary software applications are described based on the physical location of the data within the specific application. This is true with large enterprise resource planning (ERP) tables, data cubes, and even spreadsheets (e.g., D10/G10). As a result, analytical formulas are opaque, not sharable across applications, and costly to manage. Accountants spend significant resources rebuilding common analytical formulas across common spreadsheet applications and disparate software applications just because the information is physically located in different positions in each application.
- *Controls are embedded within applications.* Similar to the limitations of physically defined analytical formulas, automated controls are applied to data contained within specific software applications. Enterprise environments that have disparate applications containing operational and reporting data—and all do—require either the redundant application of controls across the full range of disparate applications and/or the migration of data to specific software applications (e.g., the global data warehouse) for application of controls.
- *Relationships are implicit.* Relationships between business information concepts and the relevant company policies, reporting standards, auditing

standards, instructions, regulation, and so on are all implicit. Experienced management accountants, CPAs, and managers have developed their understanding of company-specific policies, GAAP standards, regulations, laws, and generally accepted auditing standards (GAAS) requirements related to specific reporting issues based on their years of experience. Inexperienced accountants, managers, investors, creditors, and other users with limited knowledge of these policies, standards, laws, and regulations may be unaware of or confused about these implicit relationships.

- *Opaque validation and business rules.* In today's business reporting and compliance processes, validation and business rules are opaque and not sharable between software applications. This results in compliance processes wherein validation and analysis typically become the user's problem. This situation results in redundant cyclical information exchanges between users and preparers as the cycles of error identification/error correction and analysis/question/answer continue until an acceptable solution is found.
- *"Spreadsheet hell."* The incredible flexibility of electronic spreadsheets has solved many business reporting problems; this flexibility has also created many new problems. Spreadsheets enable data aggregation and analysis for many business processes. Spreadsheets can also be used to eliminate a lot of rekeying and recalculating, but they are often difficult to control and manage in highly dynamic processes where the input processes are manual. Also, linking models together is not sustainable in a dynamic process. Adding one row or one column breaks the relationships between relevant data and the physically defined analytics.

In sum, internal and external reporting processes are severely affected by these constraints, all of which stem from the inability to reuse information across a wide range of disparate software applications. The XBRL standard was specifically designed to address these constraints and improve reporting processes and their associated controls.

(a) WHAT XBRL DELIVERS. Leveraging the XBRL standard, companies can more cost-effectively create efficient and flexible internal and external reporting processes that are not subject to the constraints discussed in the preceding paragraphs. By harnessing the power of standardization, XBRL provides a way to describe:

- Business information for external reporting purposes
- Business information for internal reporting purposes at the general ledger, subledger, and transaction ledger levels
- Validation, analytical, and other business rules
- Entity definitions and relationships between entities

- Relationships between business information and other relevant resources (e.g., company policies, reporting standards, regulations, references, and many other resources)
- Presentation and labeling alternatives

As a consequence of these attributes, XBRL creates an information processing environment that has the following benefits:

- *Universal information reuse.* Business information represented in XBRL is easily reusable across compliant software applications. Information can be moved from one application to another in a seamless manner. This enables the minimization of pervasive manual, costly, untimely, and complex compliance and analysis processes currently used as information is transferred from one application to another.
- *Interoperable business information concepts.* Company standardized general ledger and corporate entity concepts are applied across the full range of disparate software applications within the enterprise and even across the company's entire supply chain. The universal interoperability of these concepts dramatically increases the breadth, depth, and timeliness of information available for management decision making and the efficiency of the processes that rely upon this critical information.
- *Universal and transparent analytical rules and formulas.* Analytical and validation rules and formulas are articulated in a universal and transparent manner and executable across a wide range of software applications. This enables consumers to articulate not only their information needs but also their validation and analytical rules in a manner that is transparent and executable by preparers. This not only enables consumers to access the information in a more complete, accurate, timely, and cost-effective manner, but also enables them to share their analytical modeling concepts (e.g., macros) with other analysts, thereby providing a more relevant and richer analytical environment.
- *Centrally managed controls.* Managers should anticipate that controls articulated in a universally reusable manner can be centrally and transparently managed and executed across all the disparate applications in the enterprise. This provides a dramatically more adaptable control environment, as well as one that is both more structured and transparent, thereby enabling more automation in its architectural constructs and assessments.
- *Explicit relationships.* Relationships between business information concepts and the relevant company policies, reporting and auditing standards, instructions, regulations, company policies, and so on are all explicit and executable by disparate software applications. Any user and consumer of business information can transparently access contextually relevant policies, standards, instructions, regulations, expertise, and the like.

- *Transparent validation and business rules.* Validation and business rules are transparent, sharable, and executable across disparate software applications. This enables streamlined compliance and risk management processes wherein validation and analytical rules are developed by users and shared with and executed by preparers. Higher data quality and analysis result from the preparer providing the requested information in accordance with the specifications of the user's request. Manual data correction and analysis requests are minimized by the preparer's ability to provide the requested information the first time, thereby eliminating the cycles of error identification/error correction and analysis/question/answer between users and consumers.
- *"Spreadsheet heaven."* Electronic spreadsheets leveraging the capabilities described here will behave more like self-populating modeling and visualization platforms than manual worksheets. Spreadsheets using these features can share analytical formulas, controls, and data from across a very diverse set of information sources. In addition, not only can these spreadsheets receive exports from any ERP warehouse, they can also provide analysis and calculation functions where the results, after review, are automatically uploaded back into the proper ERP platform. This will provide a more controlled and documented audit trail along the way.

25.6 ADDITIONAL BENEFITS FROM XBRL

The standardized internal reporting process environment creates additional advantages and capabilities:

- *Leverage existing ERP systems.* A somewhat ironic fact of ERP today is that many enterprises have multiple enterprise planning systems for a wide variety of reasons. There might be different versions of an ERP system from the same vendor. The traditional approach to integrating multiple ERPs to have a "true ERP" is to add layers of ERP software on top of what already exists. XBRL makes it possible to achieve the same level of integration in a much quicker and cheaper way. For example, Wacoal, a Japanese apparel manufacturer with operations in 23 countries, leveraged XBRL in 2003 to breathe new life into 32 old and disparate ERP systems by creating a "virtual warehouse" for about one-sixth of the cost and in about one-third of the time that would have been required to create an actual global warehouse.
- *Reduce costs of future ERP investments.* Standardization at the information layer rather than the software layer provides greater flexibility in changes to and lowers future investments in the underlying software applications.
- *Lower reporting and compliance costs.* Standardized information, processes, and rules drive significantly lower internal and external reporting and compliance costs. On December 11, 2006, at the American Institute of Certified Public Accountants (AICPA) SEC and Public Company Accounting

Oversight Board (PCAOB) Update Conference held in Washington, D.C., John Stantial, director of financial reporting at United Technologies Corporation, outlined his plans to reduce reporting time and costs by 20 percent via XBRL-enabled process enhancements. And this from a company with one of the largest and most successful Hyperion installations in the world.

- *Improve decision making.* Standardized processes enable greater degrees of automation and information flow, thereby significantly increasing the timeliness, accuracy, and completeness of information available for management decision making. In addition, the scope of information from outside the company is dramatically expanded, as any internal or external information source exposed via a Web service and published in the XBRL standard can be immediately included in management's analysis.

XBRL is now sufficiently developed that companies can use it today for internal purposes. For example, the XBRL Global Ledger Taxonomy provides a powerful platform on which to create a standard chart of accounts. A diverse range of tools is also available, with more being introduced to the market every month.[10] Furthermore, numerous implementation case studies are available on the XBRL web site[11] discussing the application of standardization to eliminating the constraints discussed earlier that are occurring at virtually every segment of the business reporting supply chain.

The additional benefits of XBRL outlined here are only the beginning of how a large number of stakeholders can take advantage of this powerful new information standard. Analysts and investors will be able to perform much more sophisticated benchmarking analyses comparing companies' financial and market performances. Executives will be able to do the same with their performance vis-à-vis their major competitors.

Internal and external audit processes will be greatly enhanced, and the accounting profession is already exploring the implications of XBRL for audit methodologies. Importantly, this includes being able to do a better job of detecting accounting anomalies and unusual and other types of inappropriate transactions and ledger activities.

XBRL also has an important contribution to make to the acquisition and analysis of contextual information, such as provided in the U.S. 10-K and the International Accounting Standards Board (IASB)'s Management Commentary, and the growing interest in nonfinancial information. The latter includes both industry-specific key performance indicators (KPIs) upon which future performance depends and corporate social responsibility or "triple bottom line" reporting that takes more explicit account of the information needs of stakeholders in addition to shareholders. Obviously, their information needs substantially overlap and all can benefit from the application of XBRL to this type of information. A notable initiative here is that of the Enhanced Business Reporting Consortium (www.ebr360.org), which is working to create market-based collaborative

working groups to develop a broad reporting framework for taxonomies of contextual information, KPIs, and other information of relevance to stakeholders. Executives are increasingly using this type of information for their own decision-making purposes, so it stands to reason that this information is of interest to external users as well.

Finally, XBRL has a key role to play in helping companies with a governance, risk, and compliance issue that is rapidly rising to the top of management and the board's agenda: the management of reputational risk. Explicit interest in this topic emerged with the global accounting scandals and business failures some five or six years ago. This interest is growing rapidly, as witnessed by a recent article in the *Harvard Business Review.*[12]

The current state of practice for measuring and managing reputational risk is at a similar stage to where operating risk was 15 to 20 years ago. It is increasingly being recognized as a risk category in its own right and must be managed as such. Doing so requires the analysis and integration of a wide range of information, both internal and external, including financial, operating, market, and even textual information found in the news media, including blogs. NewsML,[13] XBRL, RIXML,[14] and other taxonomies can be useful for all of these types of information and will help facilitate the development of analytical tools for managing this important risk.

The list of benefits and applications could go on. For now, suffice it to say that all senior executives and board members have a fiduciary responsibility to learn about XBRL and how this powerful new information standard can be used to improve the governance, risk, and compliance processes.

Notes

1. www.xbrl.org.
2. www.xbrl.org/us/us/FFIEC%20White%20Paper%2002Feb2006.pdf.
3. www.xbrl-ntp.nl/english.
4. www.corep.info/.
5. www.entemp.ie/.
6. www.cro.ie/.
7. www.bolagsverket.se/in_english/news/2007/digital_filing_070122.html.
8. www.xbrl.org/LatestNews/.
9. Projects: http://serverlab.unab.edu.co:8080/mediawiki/index.php/XBRL; general: http://en.wikipedia.org/wiki/XBRL.
10. www.xbrl.org/tools/ and www.xbrl.org/productsandservices/.
11. www.xbrl.org/XBRLandBusiness/.
12. Robert G. Eccles, Scott C. Newquist, and Roland Schatz, "Reputation and Its Risks," *Harvard Business Review* (February 2007): 104–114.
13. www.newsml.org/pages/index.php.
14. www.rixml.org/.

PART 5

ENVIRONMENTAL GOVERNANCE

CHAPTER 26

THE IMPACT OF ENVIRONMENTAL LEGISLATION ON HIGH-TECH SUPPLY CHAINS

Krishna Gorrepati
Joachim Thomas Garson

26.1 INTRODUCTION

The electronics industry underwent an important transition toward designing and selling environmentally friendly products in the past five years. This transition has been triggered primarily by the introduction of environmental legislations around the globe and market trends that demand and reward sustainable and environmentally conscious design. The earliest and the most significant of these regulations are the Restriction of Hazardous Substances[1] (RoHS) and Waste Electrical and Electronic Equipment[2] (WEEE) directives passed by the European Union. RoHS, especially, triggered extensive changes in both the design and processes involved in the manufacturing of electronic products throughout the highly dispersed electronics supply chain. Recently a number of other countries followed the stance taken by the EU and introduced similar legislations—the most significant being the one issued by China.[3]

26.2 THE ROHS AND WEEE LEGISLATIONS

The RoHS directive requires companies selling electrical and electronic products in the European Union to reduce (under published threshold values) presence of six hazardous substances from certain types of electronic equipment. These substances are:

1. Lead
2. Cadmium
3. Chromium
4. Mercury
5. Polybrominated biphenyl (PBB)
6. Polybrominated diphenyl ether (PBDE)

Some medical devices, aerospace navigational electronics, and telecommunications equipment are exempt from the RoHS directive. However, the directive requires not only computers, consumer electronics, appliances, and their components to be compliant, but also electronic equipment that is being used as part of another product. The RoHS directive went into effect on July 1, 2006.

Whereas RoHS deals with the chemical composition of products, the WEEE directive requires manufacturers of electrical and electronic equipment to implement appropriate end-of-life processes (recycling, reuse, and disposal) for their products. WEEE obliges the producer of the electronics and electrical equipment to be responsible to recover and recycle a certain percentage of the weight of products sold in the European Union. The WEEE directive went into effect in August 2005, and compliance legislations are being incrementally implemented across the European Union.

26.3 RESTRICTION OF HAZARDOUS SUBSTANCES GLOBALLY

China has recently adopted legislation that is similar to the EU RoHS directive. The Chinese legislation is especially rigorous, as it requires governmental analysis and approval of any product sold in China prior to the introduction of new products into the Chinese market. Given the rising significance of China not only as a vendor on the world's markets but also as a market to sell into, this legal requirement is considered to be a major hurdle for global electronics manufacturers.

Many other countries, manufacturers, and certain U.S. states are in various stages of creating or adopting environmental product compliance legislations. These legislations are in one way or another similar to RoHS and WEEE. Exhibit 26.1 shows important voluntary environmental standards and mandated environmental legislations that are in various stages of implementation.

While the details of these legislations would go beyond the purpose of this chapter, the key takeaway is the growing significance of environmental compliance for high-tech manufacturers. During the past year, getting into compliance with the European RoHS directive has been a top CEO agenda item for all

Legislation	Issued by
Electronic Waste Recycling Act, effective since July 2004[a]	California, U.S.
Energy using Products (EuP), expected for 2007[b]	European Union
Extended Producer Responsibility (EPR)[c]	South Korea
E-Waste Law[d]	Maine, U.S.
Integrated Products Policy (IPP), expected for 2007[e]	European Union
Registration, Evaluation, and Authorization of Chemicals (REACH), expected[f]	European Union
Recycling Registration, reduction of lead, JEITA[g]	Japan
Restriction of Hazardous Substances (RoHS), effective July 2006	European Union
Measures for Administration of the Pollution Control of Electronic Information Products	China
Waste of Electrical and Electronic Equipment (WEEE), effective 08/2005	European Union

[a]Electronic Waste Recycling Act of 2003, California—www.ciwmb.ca.gov/electronics/act2003/.
[b]Energy use in Product (EuP) Directive—http://ec.europa.eu/enterprise/eco_design/dir2005-32.htm.
[c]Extended Producer Responsibility System Korea—http://eng.me.go.kr/docs/common/common_view.html?idx=51&av_pg=1&mcode=10&classno=12.
[d]Maine E-Waste Law—http://janus.state.me.us/legis/statutes/38/title38sec1610.html.
[e]Integrated Product Policy Directive—http://ec.europa.eu/environment/ipp/.
[f]REACH Directive—http://ec.europa.eu/environment/chemicals/reach/reach_intro.htm.
[g]Japanese Green Procurement—http://210.254.215.73/jeita_eps/green/greenTOP-eg.html.

EXHIBIT 26.1 ENVIRONMENTAL LEGISLATIONS AROUND THE GLOBE

electronics manufacturers. "AMR research ... estimates the costs to mitigate RoHS and WEEE risks in the electronics industry will range from 2 percent to 4 percent of revenue from the affected product lines for the first year."[4]

(a) ROHS-COMPLIANT BUSINESS PROCESSES. The RoHS and WEEE directives have an impact on practically all aspects of sales, design, manufacturing, service, and reverse logistics operations of the electronics supply chain. (See Exhibit 26.2.) Noncompliance can result in heavy penalties and temporary withdrawal of products from markets, which can cause outsized loss of revenue and brand image in the market. The most famous example is the Sony case[5]: In the fall of 2001, Sony lost $110 million in PlayStation sales in the Netherlands, as cables contained excessive amounts of cadmium; 1.3 million PlayStations missed the Christmas business and had to be reworked, which cost another $40 million. As a consequence, Sony executed a systematic review of its multi-echelon supply chain. A more recent example is Apple's decision to stop selling some if its products in the EU market.[6]

RoHS and WEEE impact the entire product life cycle from design to disposal/recycling.

Business Process	Impact
Design	Design and qualify RoHS compliance
Procure	Purchase RoHS-compliant parts and components
Manufacture	Ensure RoHS-compliant manufacturing
Deliver	Deliver RoHS-compliant products where necessary
Recover	Recover end-of-life products
Recycle	Recycle through internal operations or partners; provide information to authorities
Dispose	Ensure compliant disposal

EXHIBIT 26.2 THE IMPACT OF ROHS AND WEEE ON BUSINESS PROCESSES

26.4 IMPACT OF ROHS AND WEEE ON BUSINESS PROCESSES AND SUPPLY CHAIN PARTICIPANTS

RoHS and WEEE impact all levels of the highly fragmented electronics supply chain, including original equipment manufacturers (OEMs), component manufacturers, foundries, board assemblers, electronics manufacturing service (EMS) providers, and original design manufacturers (ODMs). (See Exhibit 26.3.)

OEMs, among the participants of the high-tech supply chain, are the ones that are most at risk. The definition for the producer given by the RoHS and WEEE directives applies mostly to the OEMs. It is the responsibility of the OEM to make sure that all products put on the market after July 1, 2006, are RoHS compliant, regardless of the manufacturer of the finished product and supplier of components. Brand-name OEMs that sell directly into consumer channels are the most exposed to random audits and tests.

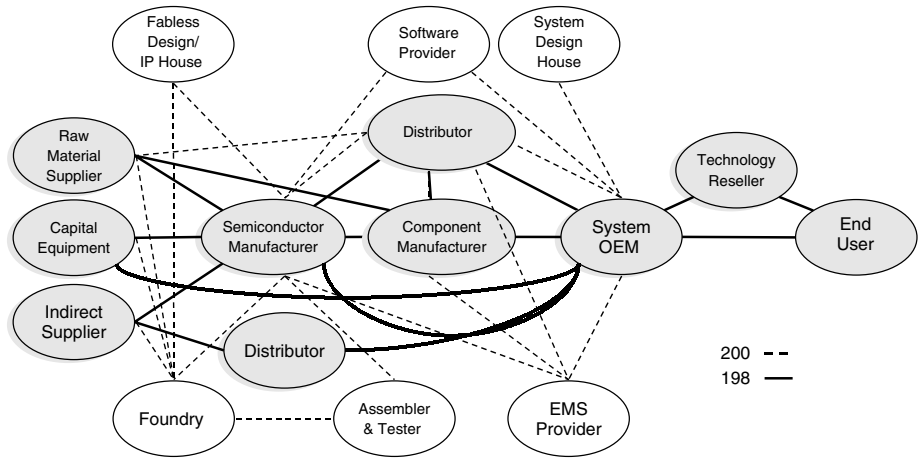


EXHIBIT 26.3 HIGH-TECH SUPPLY CHAIN

(a) PRODUCT DESIGN. Most design engineers until now have been concerned with form and function of the product or subsystem. With the passage of RoHS and WEEE directives, part of the responsibility of compliance now falls upon the shoulders of design engineers who select and integrate components into end products and subsystems. RoHS and WEEE compliance is now one of the design requirements just as form, function, and performance make up product and market requirements. Design engineers now have to use "design for environment" and "design for end of life" processes to ensure that cost-effective compliance can be achieved.

Unfortunately, design engineers do not yet have the necessary tools, information, and training to evaluate product design from the standpoint of RoHS and WEEE compliance. Innovative software companies and business process consulting companies are coming up with new applications and processes that can be used as part of new product development and logistics processes to ensure RoHS compliance and to support design for environment.

(b) PURCHASING. Purchasing managers play an important role in component and supplier selection and consequently have a significant influence on RoHS compliance. It is their responsibility to ensure that the suppliers selected for components have the necessary capacity and processes to supply RoHS-compliant parts. In addition, they should also lead the task of RoHS data collection from component manufacturers, as they have the most visibility and knowledge of component manufacturers' operations, people, and product plans.

(c) MANUFACTURING AND QUALITY CONTROL. None is more impacted by the RoHS legislation than manufacturing engineers and process engineers who have the task of designing and improving lead-free manufacturing processes. So far they have done a remarkable task of designing lead-free alloys that replace the tin-lead solder that is currently popular. The complexity, however, comes not from the alloys as much as from the higher temperature profiles of manufacturing processes and the adverse impact these higher temperature profiles have on performance and reliability of components. Furthermore, the physical fit and form of RoHS-compliant components might differ from their predecessors, causing significant redesign effort.

In addition, there is a possibility of reduced yield during the transition period due to the introduction of lead-free alloys to support electronics manufacturing processes. This has a direct impact on the cost models that EMS companies currently employ for evaluating manufacturing costs. It is likely that EMS companies have to renegotiate pricing structures with their OEM customers to accommodate reduced yields, higher rework, and increased test costs.

The quality management teams that currently ensure components meet performance, process, and logistic criteria should expand the scope of testing to check for validity of supplier declarations by conducting tests. Many of the statistical techniques used in quality control can be used to support material composition

and compliance testing. To make matters clear, government agencies and industry organizations are in the process of developing and issuing standard test procedures related to material composition and compliance.[7]

While different functional groups in the company all contribute toward RoHS compliance, the impact of the legislation on different supply chain participants varies. However, the external supply chain participants play an important role in achieving compliance.

(d) COMPONENT MANUFACTURERS. RoHS compliance places the highest burden on component manufacturers, as they are expected to minimize or eliminate the six listed hazardous substances from all components and products. They are expected to transition to RoHS compliance without changing the electronic properties of the components or sacrificing performance, while maintaining the footprint of the part. Furthermore, new compliant components have to withstand higher temperature profiles of manufacturing processes without losing performance and reliability. OEMs that design these new components into products demand disclosure of material content in the new parts and manufacturing processes and assurance that they do not contain the six listed hazardous substances. This requires additional quality control, test processes, and material composition disclosure. These new processes and customer demands increase the cost of components, and it is uncertain whether the component manufacturers can pass these costs on to OEMs.

(e) ODM/EMS COMPANIES. Over the past decade, a new breed of companies has become an important element of the high-tech ecosystem: large, full-service ODM/EMS companies. These companies offer turnkey design, manufacturing, distribution, service, and reverse logistics to OEMs. In addition, the development of the ODM model for certain product segments continues the blur organizational boundaries between OEMs and ODM/EMS companies. ODMs supply fully designed products that are relabeled by OEMs as their own products. Consequently, the OEM-ODM relationship has become more strategic and is typically based on total program management, as opposed to cost per unit.

With the introduction of RoHS and WEEE, there is now a need to reexamine traditional program management processes and enhance them to accommodate total product life cycle, exposure to noncompliance risk, processes to check and ensure compliance, and share of liability. There is a clear need to understand who bears the cost at different stages in the life cycle and how it can be allocated and recovered.

(f) SERVICE AND REVERSE LOGISTICS SERVICE PROVIDERS. In the high-tech industry, after-sales service and reverse logistics are often handled by third-party logistics and service providers. The introduction of WEEE and RoHS impacts and complicates service and reverse logistics processes. WEEE dictates that producers finance and recycle/reuse products that are recovered at the end of the

OEM	ODM/EMS	Component Manufacturer/Distributor
• Analyze all existing products and their configurations for RoHS compliance • Integrate RoHS-compliant parts into existing and new designs • Understand the effect of new parts and manufacturing processes on product reliability • Ensure product design and reverse logistics processes comply with WEEE	• Integrate RoHS-compliant parts into existing designs • Refine lead-free manufacturing processes • Reevaluate manufacturing processes to accommodate reduced yield and increased test and rework costs • Redefine program management processes to accommodate risk of noncompliance and collaborative approach to compliance	• Make RoHS material composition data available to OEMs and ODM/EMS companies • Eliminate or reduce RoHS materials in parts • If possible, ensure similar performance, reliability, and footprint characteristics

Exhibit 26.4 Impact of RoHS and WEEE on High-Tech Supply Chain Participants

product life cycle. Reverse logistics providers need to develop and refine business processes so that there is little chance of noncompliance, specifically of the WEEE directive.

In addition, service providers should expect higher incidences of failure during the transition to RoHS compliance due to loss of reliability with new materials and new manufacturing processes. There may be a need to reprice warranty policies as well as adjust stocking policies for service parts.

Overall, the RoHS and WEEE directives push the electronics supply chain to embrace life cycle engineering as the basis for product development. Exhibit 26.4 gives a summary of issues that need to be addressed by various constituencies and functional groups.

(g) IMPLEMENTATION OF BUSINESS PROCESSES TO COMPLY WITH ROHS AND WEEE. The primary focus of RoHS compliance processes is to ensure that the products sold in the EU do not have the hazardous substances listed in the directive beyond the specified thresholds. The RoHS directive specifies the hazardous substance threshold at the homogeneous material level. A component can consist of several homogeneous materials. Electronics equipment producers have to exercise control and compliance throughout the electronics supply chain since they purchase the majority of the components used to manufacture

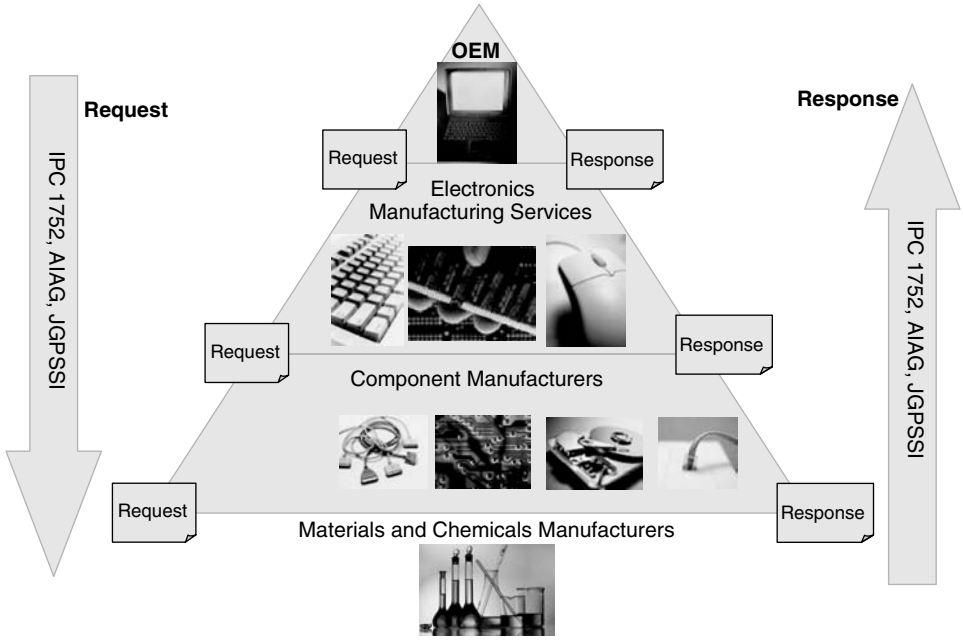


EXHIBIT 26.5 DATA EXCHANGE BETWEEN SUPPLY CHAIN PARTNERS

electronic equipment. In some cases the need for data collection and certification of compliance can ripple down to the raw material suppliers, as shown in Exhibit 26.5.

Standards such as the Institite for Printed Circuits (IPC) Material Declaration IPC 1752, the Automobile Industry Action Group (AIAG), and the Japan Green Procurement Survey Standardization Initiative (JGPSSI) have been developed by different industry groups to simplify the process of requesting and responding to compliance and composition information between supply chain partners.

However, the enforcement of incompatible compliance legislations by different countries and regions adds complexity to the process. For example, while the EU relies on self-policing and random audits as a method to enforce and test RoHS compliance, China requires testing, declaration, and labeling prior to selling products in China.

Finally, the OEM should also analyze the product for WEEE relevance and institute appropriate processes that can assure compliance. The major requirement of WEEE is that the producer finances and accounts for recovery of the product at the end of its life cycle. Although a few EU countries like Germany[8] and Austria have established business processes to support WEEE reporting, many of

the other EU countries are still in the process of implementing WEEE policies and processes.

For example, in Germany it is now sufficient to provide periodic reports based on the amount of WEEE (in weight units) that the producer places on the market. In addition, producers are expected to pay a fee for the given period. Most countries are formulating similar approaches to account for the WEEE in their distinct markets. It is likely that these processes will be amended to get a clearer idea of the impact of WEEE on the environment and how producers are accounting and paying an equitable amount to country authorities.

(h) IMPACT ON THE IT INFRASTRUCTURE. Considering the fact that most of the operations of OEM/ODM/EMS companies rely on a variety of operational systems such as ERP/PLM/SCM, it is only natural to expect changes to be made or new systems to be implemented to the landscape to support RoHS and WEEE compliance. Our analysis indicates that the following five activities and processes are needed to ensure compliance:

1. Collaborate efficiently to obtain accurate component-level data from component manufacturers.
2. Evaluate all product configurations and manufacturer combinations for environmental compliance.
3. Enhance business systems to accommodate WEEE-related reverse logistics processes, reporting to government agencies and cost accounting.
4. Accumulate and report on operational RoHS and WEEE compliance.
5. Prepare and support holistic "design for environment" process that can be used by design, product engineering, supply chain management, and reverse logistics teams.

26.5 SUMMARY

Whereas other industry segments like chemicals, energy, and utilities have had to deal with environmental regulations for a long time, environmental product compliance is a relatively new requirement for the high-tech industry. The horizontal nature of the business and dynamic pace within the industry add an additional layer of complexity to the topic of product compliance that is not normally observed in other industries.

As governments and the high-tech ecosystem gain a better understanding of the impact of RoHS and WEEE regulations, we can expect comparable regulations to emerge from other countries and regions in the world. The adoption of environmental regulations similar to RoHS and WEEE in China gives a clear indication of where major economies of the world are headed. Additional regulations such as Energy-using Products (EuP) and Integrated Product Policy (IPP) will become increasingly common and will influence every aspect of bringing products to global markets.

Companies should pay close attention to these upcoming regulations and prepare proactively to address and comply with them. The normal tendency to be complacent could force companies to withdraw products from lucrative markets. The impact of noncompliance in the form of lost market share and sales and negative brand image is a serious consequence that most companies cannot afford to entertain. Despite its disruptive effect on electronics manufacturers, the emergence of RoHS and WEEE directives around the globe helps manufacturers and their global supply chain partners in their role as responsible corporate citizens.

Notes

1. RoHS Directive: http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_037/l_03720030213en00190023.pdf.
2. WEEE Directive: http://ec.europa.eu/environment/waste/weee_index.htm.
3. Measures for Administration of the Pollution Control of Electronic Information Products: http://english.mofcom.gov.cn/aarticle/policyrelease/domesticpolicy/200605/20060502132549.html.
4. *Economist* Intelligence Unit, "Efficient Compliance with Environmental Rules in the High Tech Industry," February 2006.
5. "Sony Swaps PlayStation One Cables," CNet News, December 2001, http://news.com.com/2100-1040-276646.html?legacy=cnet.
6. Katie Marsl, "Apple to halt sale of some products in Europe," Apple Insider, June 21, 2006.
7. IEC TC111 WG3: Test Methods for Detection of Hazardous Substances and Compliance, www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=2814.
8. EAR Germany: www.stiftung-ear.de/content/e47/e922/050909RoadmapRegistration_ger.pdf?preview=preview.

CHAPTER 27

ENVIRONMENTAL COMPLIANCE AND ENFORCEMENT IN CHINA

Wanxin Li, PhD
Krzysztof Michalak

27.1 INTRODUCTION

On April 14, 2006, in his address to the Sixth National Conference on Environmental Protection, Premier Wen Jia-bao of China alerted the country to give environmental protection a higher priority and fight against worsening environmental pollution and ecological deterioration.[1] Before the environmental degradation and ecological/economic/health loss became a topic of national focus, China has, since early 1970s, incrementally established the legal and institutional frameworks aiming to control pollution. Enforcement of environmental laws and standards and compliance promotion instruments utilized by government decide, to a large extent, industrial environmental performance and thus national environmental performance. In this chapter, pressures on the environment will first be reviewed, followed by responses from government and society—institutional and legal framework of the existing enforcement and compliance system; the current

status of environmental enforcement and compliance promotion comprises the following section; next, compliance by industry will be evaluated. Rising public environmental awareness that will potentially change the power distribution of the enforcement game, and its implication for the national goal of constructing a harmonious society will end this chapter.

27.2 PRESSURES ON THE ENVIRONMENT

With 1.3 billion people, comprising 20 percent of the global population, China only has only 6.8 percent of global arable land. The desire for self-sufficiency has exerted large pressures on the ecosystem. For example, because sparrows were thought to compete with humans for food, Chairman Mao Tse-tung called forth a national campaign in 1958 aiming to kill off the birds in China. As a result, we can rarely see sparrows and it is now one of the endangered species in China.

Starting in the early 1990s, the processes of industrialization and urbanization have generated pressures on the environment as well. Between 1979 and 2005, the average gross domestic product (GDP) growth rate in China was 9.3 percent annually. Urban population increased by 4.2 percent annually between 1990 and 2003, with a total of 523.8 million in 2003, accounting for 40.53 percent of the total population in China. The expanding scale of industrial and human activities and associated material flows have caused resource depletion and created wastes beyond the assimilative capacity of the environment.

As a result, China's environment has become a significant issue both domestically and internationally. In her testimony to the Congress of the United States, Elizabeth Economy (2004a) said, "Yet this [rapid] economic development, coupled with a weak enforcement apparatus for environmental protection, has also resulted in a range of devastating consequences for the environment."[2] Air and water quality degradation, deforestation, and soil erosion are only a few items on a long list of environmental challenges facing China today.[3]

Widespread air pollution in China has caused the worst health damage and economic loss in the world. In 2000, China had 16 of the 20 most polluted cities in the world.[4] About 63.5 percent of China's cities suffer from medium to severe air pollution. By 2020, China will have 110 million cars, accounting for over 60 percent of air pollution in cities.

The most serious problem facing China probably is access to water. Nationwide per capita water supply is about 2,300 cubic meters per year, which is only a quarter of the world average. Water pollution made the already short water supply even worse. Approximately 700 million people drink contaminated water on a daily basis. In rural areas, to maximize agricultural production, Chinese farmers have practiced intensive farming and applied unnecessarily large amounts of fertilizer and pesticide. Agricultural runoff has made a lot of local waters biologically dead. Associated with the urbanization process, sewage discharge in Chinese cities has been increasing by 5 percent annually. But less than 40 percent of municipal wastewater discharge received primary treatment in 2005.

Besides air and water pollution, China faces other environmental challenges as well. Desertification has caused sandstorms that have had impact beyond national borders. For example, in 2000 China had its worst sandstorm to date, and neighboring countries such as Japan and South Korea complained that the sand from China had made their air dirty. In 2002, Beijing had 12 occurrences of sandstorms, whereas the annual average had been only 1.7 between 1950 and 1990. Many endangered species are threatened; one of the most biologically rich regions in Asia, the Tiger Leaping Gorge (a UNESCO Natural Heritage Site) is being threatened with a series of eight dams.

In 2005, by purchasing power parity, China became the second largest economy in the world, but its GDP per capita was only $1,820. In the foreseeable future, economic growth will still be a major task of the Chinese government. So the ability to strike a good balance between aggressive environmental enforcement and compliance work and the pursuit of economic wealth is critical to China's sustainable development.

27.3 LEGAL FRAMEWORK

Starting from the mid-1970s, after China participated in the 1972 United Nations Conference on Human Environment held in Stockholm, the leadership of China has begun to realize the importance of the environment for economic and social development. During the past 30 years, China has established from scratch comprehensive environmental standards and regulations (see Exhibit 27.1); built up administrative institutions; trained professionals in environmental policymaking, law enforcement, and scientific research and development; and worked in collaboration with international organizations, intellectuals, and foreign governments to combat environmental problems in China.[5]

The Chinese Constitution specifies a positive role of the state in protecting the public from pollution and other hazards.[6] The Chinese government promulgated its first trial version environmental protection legislation, the PRC Environmental Protection Law, in 1979. At present, this framework includes roughly 22 statutes, more than 40 regulations, approximately 500 standards, and more than 600 other legal norm-creating documents primarily addressing pollution control, natural resource conservation, and management of the environmental stewardship aspects of consumer products (product stewardship). At the local-government level, one senior environmental official indicated that environmental measures at the provincial and municipal levels alone likely total more than one thousand.[7]

Two principles have guided the design of the environmental regulations and policies in China: pollution prevention and polluter pays.

27.4 INSTITUTIONAL FRAMEWORK

In the development of the environmental regulatory system, the Chinese government has constructed the institutions to carry out the policy mandates.

Year	Regulations on Pollution Prevention and Control
1979	PRC Environmental Protection Law (amended 1989 and 2001)
1982	Marine Environmental Protection Law (amended 1999)
1982	Collection of Pollution Discharge Fees
1984	Water Pollution Prevention and Control Law (amended 1996)
1987	Air Pollution Prevention and Control Law (amended 1995 and 2000)
1995	Solid Waste Pollution Prevention and Control Law
1995	Provisional Regulations on Huai River Basin Water Pollution Prevention and Control
1996	Environmental Noise Pollution Control Law
2002	Environmental Impact Assessment Law
2002	Cleaner Production Promotion Law
2003	Ordinances on Collecting and Managing Pollution Discharge Fee
2003	Radioactive Pollution Prevention and Control Law
	Regulations on Natural Resources and Ecosystem Integrity
1984	Forestry Law (amended 1998)
1986	Grasslands Law
1986	Land Resources Law (amended 1998)
1986	Fisheries Law
1986	Mineral Resource Law (amended 1996 and 1999)
1988	Wildlife Protection Law
1988	Water Law (amended 2002)
1991	Water and Soil Conservation Law
1993	Water and Soil Conservation Law Implementation Regulations
1994	National Park Regulations
1996	Natural Flora Protection Regulations
1997	Energy Conservation Law
1997	Flood Prevention Law
2001	Law on Desertification Prevention

EXHIBIT 27.1 ENVIRONMENTAL REGULATIONS IN CHINA

- In 1974 the Environmental Protection Bureau with 20 staff members was established under the State Council.
- In 1982 the Division of Environmental Protection with 60 staffers was established within the Ministry of Urban and Rural Construction and Environmental Protection.
- In 1988 the Environmental Protection Commission was created within the State Council to enhance interministerial coordination on environmental protection.
- In 1988 (the same year) the National Environmental Protection Agency (NEPA) with 320 staff members was created.
- In 1998 NEPA was elevated to a ministerial level and renamed the State Environmental Protection Administration (SEPA), but the State Council's Environmental Protection Commission was dismantled.

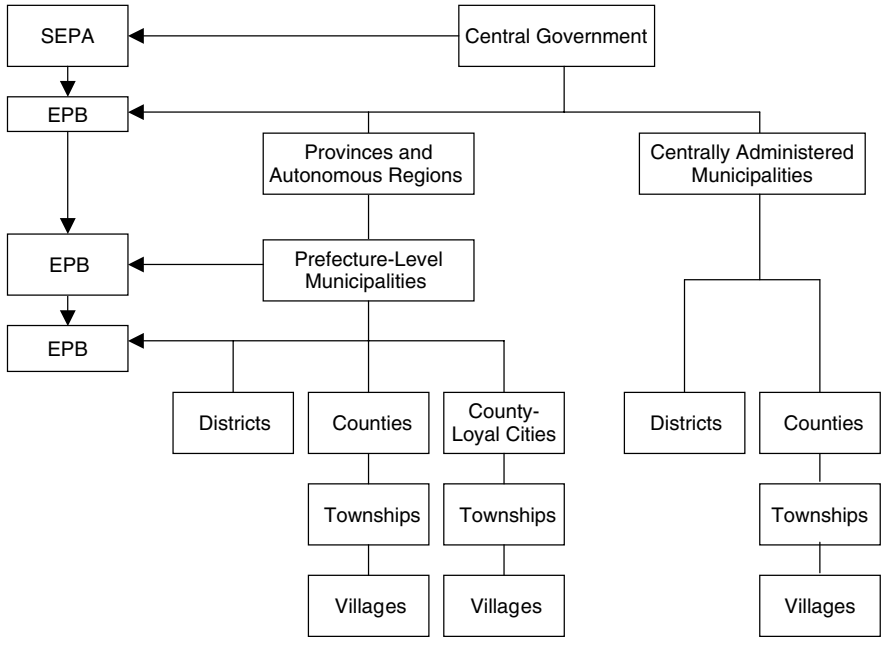


EXHIBIT 27.2 STRUCTURE OF GOVERNMENT ADMINISTRATION IN CHINA

Under SEPA, there are three levels of local environmental protection bureaus (EPBs): provincial, city/county, and district. Local EPBs are the agencies chiefly responsible for regulatory enforcement. Although they are nominally affiliated with SEPA, local EPBs are first and foremost subordinate to local governments. (See Exhibit 27.2.)

As such, they depend on local governments for funding and personnel. Furthermore, they must compete with other government agencies—for example, industrial bureau, economic bureau, and so on—for funding and influence. Because local government officials are generally compensated and rewarded for the rate of GDP growth of their jurisdictions, they typically place economic advancement before regulating industry.

Under the dual command of SEPA and their local governments, local EPBs frequently lack the resources and leverage needed to translate regulatory promise into environmental progress. Environmental monitoring and enforcement are consequently rather weak.

27.5 ENFORCEMENT AND COMPLIANCE PROMOTION

(a) TOOLS AT DISPOSAL OF GOVERNMENT. To give teeth to the standards and environmental regulations in China, SEPA has adopted a comprehensive system of policy instruments to prevent and control pollution. (See Exhibit 27.3.)

Category	Environmental Protection Policy Instrument
Preventive	Three simultaneous measures: Environmental impact assessment Cleaner production Circular economy
Direct regulation I (administrative)	Limited time treatment Discharge permit
Direct regulation II (economic)	Pollution levy/pollution discharge fee
Incentive mechanism I (economic)	Tradable emissions permit
Incentive mechanism II (information)	Color rating and disclosure of environmental performance of firms Disclosure of important pollution sources
Incentive mechanism III (political)	Comprehensive evaluation of city environmental protection Environmental responsibility system Environmental protection model city/township/village National model eco-park Eco-village
Voluntary approaches	National environmentally friendly enterprises ISO 14000

Exhibit 27.3 Environmental Protection Policy Instruments in China

More specifically, there are four major policies aimed at preventing pollution: three simultaneous, environmental impact assessment, cleaner production, and circular economy. Three different types of pollution control instruments have been adopted: direct regulation, incentive mechanisms, and voluntary approaches. Within the category of direct regulation, three policy instruments are included: limited time treatment, discharge permit, and pollution levy/pollution discharge fee.

With less government direct intervention, incentive mechanisms motivate government officials and industry people to pursue better environmental results, which are in their self-interests as well. Three incentive mechanisms are at work: economic, informational, and political. More specifically, tradable emissions permits work through calculations of economic gains/losses by polluters. Color rating and disclosure of environmental performance of firms or disclosure of important polluting sources align stakeholder interests through making environmental information publicly available. Comprehensive evaluation of a city's environmental protection, environmental responsibility system, or environmental protection model city motivates government officials, partially because it may affect advancements in their political careers. Voluntary approaches are relatively less developed in China with only two instruments in the tool kit: the naming of nationally environmentally friendly enterprises by SEPA and certifying with the ISO 14000 of individual enterprises.

(b) ADMINISTRATIVE DISCRETION BY LOCAL EPBS AND GOVERNMENTS. First of all, officials of local EPBs and local governments enjoy a large degree of discretion in environmental monitoring and enforcement. The Chinese national environmental regulations are usually worded generally and are defined by officers in the field. For example, to implement SO^2 emissions trading, local EPBs have to first specify the total amount of sulfur dioxide dischargeable to an area in the upcoming five years, then allocate it to coal-fired power plants and other SO^2 producers, and further keep track of SO^2 emissions and transactions among polluters. Defining an allowable total emission is more an art than a scientific issue, especially as SO^2 travels across regions and the monitoring of sulfur dioxide emissions even within regional boundaries is far from accurate.

Moreover, local governments will intervene in the work of their EPBs when there is a conflict of interests, and the will of the local governments generally prevails. The discretion by local governments sometimes hinders their EPBs from exercising their discretionary authority in a good way. For example, some local governments would protect an industry that was profitable but highly polluting and did not allow information on its environmental performance to go public.

In short, although environmental regulations are enacted by the central government and are uniform across the country, the discretion by local EPBs means there are numerous idiosyncratic working programs in practice in China.

(c) WEAK ADMINISTRATIVE CAPACITY OF LOCAL EPBS. Assuming the goodwill of local EPB officials, administrative discretion can be good and necessary if they have the capacity to accurately target bad guys, especially since local EPBs have only limited regulatory resources. Otherwise, wide administrative discretion introduces capricious government actions, favoritism to special interests, and corruption.[8] In practice, it is widely acknowledged that administrative capacity of local EPBs is insufficient.[9] Lack of necessary financial and human resources and a resulting displacement of goals comprise the major causes. For example, continuous monitors are very important for compliance assurance by constantly putting industry on the defense. However, because of a lack of funding, even in regions such as Jiangsu Province where the local economy is well developed, not every EPB is equipped with continuous monitors.

Besides insufficient technology and equipment, the quality and quantity of the human capital employed by local EPBs pose another constraint on accurate monitoring and aggressive enforcement. Provincial average percentages of professional employees of local EPBs are generally low across China. In 2002, they ranged from the lowest, 16.3 percent in Tibet, to the highest, 74.7 percent in Beijing, with a national mean of 53.3 percent. An average local EPB in China employed 13.3 staff members in 2002, with the least (6.4) in Qinghai and the most (24.1) in Henan.[10]

Even though staff size is small, local governments cover only a fraction of the staff salary and operational costs of their EPBs. Local EPBs and

their monitoring stations have to earn revenue to supplement their income by conducting contracted work for industry. However, the conflict of interest puts professional impartiality at stake and consequently the accuracy of environmental information is sacrificed.[11]

Overall, the capacity of local EPBs to pick up signals is lacking because of a shortage of administrative stock (financial and human capital, technology, and equipment) and sometimes conflict of interest. To cope, local EPBs have adopted a targeted enforcement strategy of following up on citizen complaints. Unfortunately, the enforcement is sometimes biased because citizens usually do not have the technical knowledge to assess environmental harm and risks, and regulatory resources tend to be allocated more to issues that are more visible.[12]

(d) INCENTIVE MECHANISMS TO ALIGN INTERESTS OF GOVERNMENTAL OFFICIALS. Besides the structural barrier to vertical coordination on and horizontal integration of environmental protection work (*tiao-kuai*) and weak administrative capacity of local EPBs, the evaluation and reward system that is purely focused on the GDP growth misaligns the interests of local government officials. As a result, the desire for economic growth always outweighs environmental considerations in development decision making.

Although some environmental policies are intended to motivate government officials by naming their cities/counties as "national model city for protecting the environment," "eco-city/county/village," and the like, only regions that want to become environmental leaders respond to the political incentives. For example, in 2002, Zhenjiang, Jiangsu Province decided to compete for the title of "model city for protecting the environment" and thus significantly increased the budget of its monitoring station. Between 1994 and 2002, the annual budget of the Zhenjiang monitoring station had stayed at a 4 million yuan level. It could just meet daily operational needs but with no money left for upgrading equipment or expanding monitoring services. Since 2003, its budget has been greatly increased. The 2003 budget was 4.8 million yuan; the 2004 budget became 7 million yuan with 4 million to be set aside for purchasing new monitoring equipment; the 2005 budget was further increased to 9 million yuan, with 5 million for conducting special environmental surveys. In 2004, Zhenjiang was named a "model city for protecting the environment" by SEPA.

The Zhenjiang example illustrates that local governments could make a credible commitment to protecting the environment. If political incentives at work are pro environment and resources are available, government officials would have the political will to carry out government actions forcefully toward a better environment. Not surprisingly, other types of environmental policies, such as preventive measures, command-and-control environmental policies, and economic incentive mechanisms, tend to work better in jurisdictions where the local governments have such a political will.

Unfortunately, environmental monitoring and enforcement are problematic in jurisdictions that do not want to pursue environmental excellence.

27.6 COMPLIANCE BY INDUSTRY

The level of compliance by enterprises with pollution standards, permits, and payment of charges is checked through environmental inspections carried out by inspectors from EPBs. Private enterprises are inspected by the EPB of the jurisdiction where they are located. Each EPB maintains a list of enterprises that pose threats to the environment. Each year, EPBs conduct more than 2 million inspections. EPBs send out inspectors for conducting regular, but also surprise, site visits. The 2001 Administrative Penalty Procedures set forth guidelines for national and local enforcement staff for establishing and investigating noncompliance and applying enforcement actions to violations of national and local environmental law. When noncompliance is established, inspectors can issue warning letters, impose fines, or withdraw the permit for a part of or the whole installation.

Different levels of EPBs have different responsibility and authority to impose penalties. County-level EPBs can impose fines of up to CNY 10,000, city EPBs can impose fines up to CNY 50,000, while provincial and centrally administered municipality EPBs can impose up to CNY 200,000. The determination of a level of a fine is subject to the discretion of the local government, but the decision-making should be "open and fair." The severity of the penalty can be adjusted by taking account of such factors as the degree to which regulations were violated, the number of times the violation occurred, and the response to the violation (whether voluntary corrective action was taken). Fines are also levied by the National Development and Reform Commission (NDRC) in cases of serious breaches of the law.

Compliance promotion in China is much less developed than punitive measures. The government has at its disposal only limited tools to promote compliance and good environmental performance and does not actively reach out to regulated entities to inform them of developments in environmental regulations. To most polluters, only fines or other punitive measures are evidence of the government's concern about industry's environmental performance.

27.7 RISING PUBLIC ENVIRONMENTAL AWARENESS

The Chinese public is well aware of environmental problems. In 2005, 94.9 percent of the public thought environmental problems in China were very serious and urgent.[13] About 70 percent of the public was unsatisfied with their local environmental conditions. About 26 percent of the public thought the quality of their local environments in 2005 was worse than it was five years before, compared with about 22.5 percent of the public who thought so in 1999. This means the public has recognized pollution to be a serious problem in their daily lives.

As to the most urgent environmental problems, the public came up with the following listing in an order of perceived importance from the most to the least:

drinking water security, air pollution, domestic solid waste discharge, industrial solid waste discharge, desertification, water supply shortage, noise, and exhaust from motor vehicles.[14]

In 1999, over one-third of the government officials and entrepreneurs thought agriculture was not a major cause of environmental degradation in China.[15] In contrast, in 2005 pollution in rural areas caused by agriculture and township/village enterprises (TVEs) was recognized to be a serious problem by both experts and the rural residents. The experts identified the treatment of pollution from diffuse sources to be the fourth priority after industrial pollution, municipal wastewater, and pollution by TVEs. A higher percentage of rural people than urban residents felt their local environmental quality had degraded.[16]

It is clear that the Chinese people, both rural and urban, are well aware of environmental problems, and the level of environmental awareness has been rising. Polluters have been sued in courts more often than before even though the court usually had difficulty forcing the harm creator to compensate pollution victims. The public opinion poll has listed environmental issues to be the second most likely cause for social unrest in 2005. Protests on environmental issues in 2005 were a radical expression of rising public environmental awareness in China.

27.8 HARMONIOUS SOCIETY AND ENVIRONMENTAL COMPLIANCE AND ENFORCEMENT

China has set the goal of constructing a harmonious society. Reducing the implementation gap, in particular at the subnational level, is one of the major challenges in improving environmental performance and building a harmonious society in China. Chinese authorities have recognized this problem, most recently with the December 2005 State Council Decision on Implementing the Scientific Concept of Development and Strengthening Environmental Protection. The decision provided for strict enforcement of environmental laws and regulations and firm noncompliance response, as well as strengthening the prosecution system. It also called for greater engagement of the public in environmental compliance promotion. We can see the potential of administrative, legal, public, and industrial forces to converge to achieve better environmental enforcement and compliance in China.

Notes

1. "We must be fully aware of the severity and complexity of our country's environmental situation and the importance and urgency of increasing environmental protection. Protecting the environment is to protect the homes we live in and the foundations for the development of the Chinese nation. We should not use up resources left by our forefathers without leaving any to our offspring. China should be on high alert to fight against worsening environmental pollution and ecological deterioration in some regions, and environmental protection should be given a higher priority in the drive for national modernization."—Premier Wen Jia-bao at the Sixth National Conference on Environmental Protection on April 14, 2006.
2. Economy (2004a).

3. Responding to the severe environmental pollution and natural resources shortage, the National Environmental Protection Agency (NEPA) and the State Planning Commission (SPC) jointly proposed China's Environmental Action Plan for 1991–2000. This plan highlights the environmental issues that national officials consider particularly significant. The top three problems deal with pollution: water and air pollution and hazardous waste. The second three involve conservation of natural resources: water, land, and forests and grasslands. The final one centers on the balance and integrity of China's ecosystems. Ma and Ortolano 2000.
4. Economy (2004b).
5. Ibid.; Jahiel (1998); Morgenstern et al. (2002); Morgenstern et al. (2004); Palmer (1998); Wang et al. (2004).
6. Article 11 of the 1978 Constitution states: "The state protects the environment and natural resources, and prevents and eliminates pollution and other hazards to the public." Article 26 of the 1982 and 2004 Constitution states: "The state protects and improves the environment in which people live and the ecological environment. It prevents and controls pollution and other public hazards. The state organizes and encourages afforestation and the protection of forests."
7. Ferris and Zhang (2003); Li (2001).
8. Davis (1969); Handler (1986); Lowi (1969); Rohr (1989).
9. Interview 06072005-07. Field study by author conducted in August 2005 in Jiangsu Province, China. For example, even in a prefecture-level city in Jiangsu Province, one of the most economically advanced regions in China, not until 2004 was its EPB equipped with mobile monitoring trucks. There were no continuous monitors installed in enterprises that were connected to monitoring stations then.
10. Author calculation based on *China Environmental Yearbook 2003*.
11. Interview 06072005-07; 07182005-01.
12. Wang et al. (2003); Wang and Wheeler (2000).
13. All China Environmental Federation (2005).
14. Ibid.
15. Are the Following Parties Responsible for the Environmental Degradation in China?

Responsible Parties	Respondent	Mainly Responsible	Somewhat Responsible	Not Responsible
Industry	Government official	58.7	38.5	2.8
Industry	Entrepreneur	53.5	41.6	4.9
Local government	Government official	57.9	33.5	8.6
Local government	Entrepreneur	52.6	36	11.5
Central government	Government official	56.2	30.3	13.5
Central government	Entrepreneur	51.2	30.3	18.6
Individuals	Government official	24.3	45.7	29.9
Individuals	Entrepreneur	22.3	39	38.7
Service industry	Government official	20.5	51.8	27.6
Service industry	Entrepreneur	20.3	46.9	32.8
Agriculture	Government official	16	48.4	35.7
Agriculture	Entrepreneur	16.2	39.6	44.2

Source: Ming Yang, *Environmental Issues: Awareness and Perceptions*, vol. 1, ed. B. Zhao Beijing: Huaxia Publishing House, 2002), Table 4.2.2-1, 181.

16. All China Environmental Federation (2005).

References

All China Environmental Federation. 2005. Public comments on the eleventh five-year national plan on environmental protection in China. Beijing: State Environmental Protection Administration.

Bell, Ruth Greenspan. 2002. Institutional challenges in environmental governance: Moving beyond general principles to achieve concrete results. *RFF Issue Brief*.

Bell, Ruth Greenspan. 2003. Choosing environmental policy instruments in the real world. In *OECD global forum on sustainable development: Emissions trading/concerted action on tradable emissions permits country forum*. Paris: OECD Headquarters.

Davis, Kenneth Culp. 1969. *Discretionary justice: a preliminary inquiry*. Baton Rouge: Louisiana State University Press.

Economy, Elizabeth. 2004a. Congressional testimony: China's environmental challenges. In *Subcommittee on Asia and the Pacific; House International Affairs Committee*. Washington, DC: Council on Foreign Affairs.

Economy, Elizabeth. 2004b. *The river runs black: The environmental challenge to China's future*. Ithaca: Cornell University Press.

Ferris, Richard J., and Hongjun Zhang. 2003. Reaching out to the rule of law: China's continuing efforts to develop an effective environmental law regime. *William and Mary Bill of Rights Journal* 11:568–602.

Handler, Joel F. 1986. *The conditions of discretion: Autonomy, community, bureaucracy*. New York: Russell Sage Foundation.

Jahiel, Abigail R. 1997. The contradictory impact of reform on environmental protection in China. *China Quarterly* 149:81–103.

Jahiel, Abigail R. 1998. The organization of environmental protection in China. *China Quarterly*:757–787.

Li, Qijia. 2001. Environmental regulations in China. In *China environment and development review*, vol. 1, ed. Y. Zheng and S. Wang, ch. 20, 309–321. Beijing: Social Sciences Documentation Publishing House.

Li, Wanxin, and Eric Zusman. 2005. Institutional capacity of local EPBs and its implications for pollution control in China. In *Urban China research network annual conference—Chinese cities in transition*. Shanghai.

Lowi, Theodore J. 1969. *The end of liberalism: Ideology, policy, and the crisis of public authority*. New York: Norton.

Ma, Xiaoying, and Leonard Ortolano. 2000. *Environmental regulation in China: Institutions, enforcement, and compliance*. Lanham, UK: Rowman & Littlefield.

Morgenstern, Richard, R. Anderson, Ruth Greenspan Bell, A. Krupnick, and Xuehua Zhang. 2002. Demonstrating emissions trading in Taiyuan, China. *RFF Discussion Paper*.

Morgenstern, Richard D., Piya Abeygunawardena, Robert Anderson, Ruth Greenspan Bell, Alan Krupnick, Jeremy Schreifels, Cao Dong, Jinan Wang, Jitian Wang, and Steiner Larsen. 2004. Emissions trading to improve air quality in an industrial city in the People's Republic of China. *RFF Discussion Paper*.

Palmer, Michael. 1998. Environmental regulation in the People's Republic of China: The face of domestic law. *China Quarterly*:788–808.

Rohr, John A. 1989. *Ethics for bureaucrats: An essay on law and values*. New York: M. Dekker.

Wang, Hua, Jun Bi, David Wheeler, Jinnan Wang, Dong Cao, Genfa Lu, and Yuan Wang. 2004. Environmental performance rating and disclosure: China's GreenWatch program. *Journal of Environmental Management* 71:123–133.

Wang, Hua, Nlandu Maningi, Benoit LaPlante, and Susmita Dasgupta. 2003. Incomplete enforcement of pollution regulation: Bargaining power of Chinese factories. *Environmental and Resource Economics* 24:245–262.

Wang, Hua, and David Wheeler. 2000. *Endogenous enforcement and effectiveness of China's pollution levy system*. Washington, DC: World Bank.

Yang, Ming. 2002. *Environmental issues: Awareness and perceptions*, vol. 1, ed. B. Zhao. Beijing: Huaxia Publishing House.

CHAPTER 28

THE TRAJECTORY OF ENVIRONMENTAL REGULATION: A STRATEGIC APPROACH FOR INDUSTRY

Michael Kirschner

The electronics, automotive, cosmetics, toy, textile, chemical, and other industries are being subjected to a new strain of environmental regulations worldwide that is creating enormous challenges for them as well as substantial opportunities. This chapter covers four areas:

1. A short overview of the drivers for this new type of regulation
2. The characteristics of the resulting regulations (both current and future)
3. The impact of these regulations on the product life cycle process
4. A holistic approach to product design that enables a strategic approach to environmental regulation

28.1 DRIVERS

In late 2004 the WWF (formerly the World Wildlife Fund) published its biannual Living Planet Report.[1] According to the report, human impact on the natural environment includes a 40 percent decline in terrestrial, freshwater, and marine species populations; an increase in "energy footprint"[2] of 700 percent; an increase of human population of 65 percent; and a transition from using about half the earth's biological capacity to exceeding it by 20 percent—all over the past four

decades. Simply looking around nearly any industrialized society, one sees evidence of this in unchecked urban sprawl, increased population density, traffic congestion, overflowing landfills, increasing energy costs, and so on.

Indeed this is at a very high level, but the fact is that natural resource utilization impacts all of this, and products utilize and impact these resources in their manufacture, use, and disposal in various ways. Growth of this impact at the current rate is clearly not sustainable, so steps must be taken to rein it in with minimal impact on economic systems.

28.2 CHARACTERISTICS OF RESULTING REGULATIONS

The European Union (EU) is now the clear[3] thought leader (and certainly the most aggressive one) in taking both direct and immediate steps, as well as developing a series of long-term strategies to deal with these problems. In part this is driven by a land mass half that of the United States with 50 percent greater population, centuries of industrialization and its accompanying waste, as well as Article 6 of the Treaty Establishing the European Community,[4] which states:

> Environmental protection requirements must be integrated into the definition and implementation of the Community policies and activities referred to in Article 3, in particular with a view to promoting sustainable development.

Aggressive nongovernmental organizations (NGOs) like WWF and a government and populace receptive to environmental regulation due to a significant Green Party presence are also key factors in the EU's leadership role.

(a) THEMATIC STRATEGIES. To provide a framework for addressing these issues, the European Commission's Environment DG[5] (Directorate-General) has devised a series of seven "thematic strategies."[6] They "represent the next generation of environment policy. As their name suggests, they work with themes rather than with specific pollutants or economic activities, as has been the case in the past. They take a longer-term perspective in setting clear environmental objectives to around 2020 and will thus provide a stable policy framework. Finally, they focus on identifying the most appropriate instruments to deliver European policy goals in the least burdensome and most cost-effective way possible." The areas covered are:

- Air Pollution (adopted September 21, 2005)
- Prevention and Recycling of Waste (adopted December 21, 2005)
- Protection and Conservation of the Marine Environment (adopted October 24, 2005)
- Soil
- Sustainable Use of Pesticides
- Sustainable Use of Natural Resources (adopted December 21, 2005)
- Urban Environment (adopted January 11, 2006)

One interesting aspect of the thematic strategies, particularly the natural resources strategy, is the stated objective at the Environment DG level to influence strategies in rapidly expanding economies outside of the EU. This is more than an idle statement; the EU is actively working with China and even U.S. states (particularly Massachusetts and California) on developing similar laws by explaining their approach and coaching legislators through the thought process. The remainder of this section focuses mainly on the EU's approach, since most other recent and visible legislation and regulation around the world has to this point been patterned after it.[7]

This section also focuses, albeit not exclusively, on the electronics industry and how some policies, directives, and regulations target it in different, but complementary, ways.

(b) INTEGRATED PRODUCT POLICY. Of potentially significant interest to product industries is the EU's Integrated Product Policy (IPP).[8] While not a regulation, this policy guides the development and focus of regulation intended to drive sustainable product development. This is defined as "meeting the needs of the present generation without compromising those of future generations." One key attribute it espouses is "life cycle thinking." We discuss an approach to this in the final section of this chapter. EU directives such as Restriction of Hazardous Substances (RoHS) and Waste Electrical and Electronics Equipment (WEEE) can be considered to be within the scope of IPP and are intended to implement certain of its objectives.

Europe effectively has a multiyear lead on most other countries and regions in terms of recognizing the challenges, planning an approach, and taking action. We now see review and in some cases adaptation, for instance, of localized versions (but often with decidedly different characteristics and approaches) of the RoHS directive in China, California, Japan, Australia, South Korea, and other places.

(c) RoHS and WEEE. The European Union's RoHS directive cost the worldwide electronics industry billions of dollars to comply with. Pamela Gordon of electronics industry market research firm Technology Forecasters, Inc. found through extensive interviews with 75 electronics original equipment manufacturers (OEMs) that it has cost individual companies between 1.5 percent and 2.5 percent of cost of goods sold to achieve compliance. She further conservatively estimates the total expenditure required to comply with RoHS to have been on the order of $8 billion.[9]

What we have seen with RoHS (and the End of Life Vehicle [ELV] directive, 2000/53/EC, which focuses on automobiles and automotive electronics) is an attempt to impact the materials that electronic products are designed with. With WEEE, the target is both limiting the amount of electronic waste that ends up in landfills through both a subtle and indirect attempt to drive product design choices toward the use of more recyclable materials and improved reusability (which, given current personal computer architecture, is almost impossible to achieve with the pace of technology development—who wants to reuse a 500 MHz CPU these days?), as well as ensuring that someone has physical and fiduciary

responsibility for recycling end-of-life products rather than allowing them to enter the waste stream.

(d) ENERGY-USING PRODUCTS. EuP, the Energy-using Products directive (2005/32/EC), addresses certain classes of high-volume consumer and business products that use energy. Its goal is to drive the use of less, and less energy-intensive, materials in the product itself as well as less energy during the product's manufacturing and use. As written, the directive itself has limited regulatory impact, but any implementing measures passed could. The directive says that such measures can be avoided by industry voluntarily adopting and implementing its requirements.

The key requirement of EuP is the "ecological profile," which is a metric of how well a given product achieves these material and energy-related goals. The expectation is that consumers will use this metric, along with all the other existing attributes they already use, to select which competing product to purchase. Thus the market will drive OEMs in competitive markets to improve their products' ecological profile in order to compete. Government can also provide incentives such as reduced value-added tax (VAT) on products with an ecological profile in the top 20 percent among all similar products.

(e) REACH. RoHS targeted only six classes of substances; these equate to around 100 different substances and chemical compounds. Thousands of substances are used in electronic products, many of which are known or suspected to be toxic to people and/or the environment.

Registration, Evaluation, and Authorization of Chemicals (REACH) proposes to replace Europe's current system used for assessing the risks of existing substances (those placed on the market before September 1981) and new substances with a single regulatory framework. Today, existing substances can be used without testing and are virtually unregulated. This class of substances, numbering on the order of 30,000, represents upwards of 99.9 percent of the market volume in the EU today. Risk assessment for these is currently the responsibility of the member states, which have insufficient resources to do the work. Robert Donkers, a U.S.-stationed delegate of the European Commission, says that of 2,600 high production volume (HPV)[10] substances, only 3 percent have been fully tested. He points out that of the 3,500 new (post-September 1981) substances, of which 100 percent have been fully tested, 70 percent have dangerous properties of one sort or another.

REACH differs from the above-mentioned directives in two significant ways:

1. It targets chemical substances, not products.
2. It is not a directive; when passed it will be a regulation at the EU level and will be immediately in effect in all EU member states. A European Chemicals Agency will be established to oversee its implementation.

REACH requires registration of all chemical substances put on the market in the EU in excess of 1 ton per year, namely the 30,000 substances mentioned

earlier. It moves the responsibility for assessing the safety of substances from the government[11] to industry and the producer(s) of the substances. Information about substance properties and use is to be shared down, up, and in some cases even between competitors[12] in the supply chain.

Evaluation is a quality check and is done randomly on at least 5 percent of all dossiers registered, and for all testing proposals for certain tests. Substances may also be evaluated in case of a suspicion that the substance presents a risk to human health or the environment.

The authorization system addresses substances of very high concern, namely those that are classified as CMR, PBT, or vPvB.[13] Substances of an equivalent concern having serious and irreversible effects to human health and the environment will also require authorization. Authorization will be provided only for specific uses of these substances where the risks are "adequately controlled" or justified by socioeconomic grounds, having taken into account the available information on alternative substances or processes. Donkers estimates that fewer than 2,000 substances will be subject to authorization.

REACH went into force on June 1, 2007. The chemical industry and even the U.S. government[14] have fought a bitter but most likely futile battle against it.

(f) OTHER IMPORTANT RECENT REGULATORY ACTIVITIES. In 2005 Europe banned the use of certain phthalates (plasticizers) in toys and child care items for infants and toddlers under three years of age.[15] Similar regulation failed in California in 2005, and legislation in Maryland proposing to ban these phthalates as well as bisphenol A (used in thermoset epoxy resins) stalled. But in San Francisco, a local ordinance passed in June 2006 that bans the offending phthalates and bisphenol-A for the crib set.[16]

In California, a March 2006 report that had been commissioned in 2004 by the state Senate Environmental Quality Committee[17] identified serious failures of national and local chemical regulation to control toxic substances consistent with what drove the EU to develop REACH. It recommends that California move forward with developing a modern, comprehensive approach to chemical regulation and management that also is fundamentally oriented toward motivating business to invest in the development and use of materials that are safer for biological and ecological systems, known as green chemistry.

The greatest wildcard of all of the regulations mentioned is REACH. Its potential to restrict or even ban substances that have been in common use for decades may impact many industries in unpredictable ways.

28.3 THE IMPACT

If we map these regulations and directives against the phase of the electronics product life cycle they impact the most, it might look something like Exhibit 28.1. This shows a typical simplified product life cycle (through phase 5a) and a simple equipment-use life cycle (phases 4b and 5b) against the intended impact of the initiatives described earlier. The picture is one of a relatively complete approach

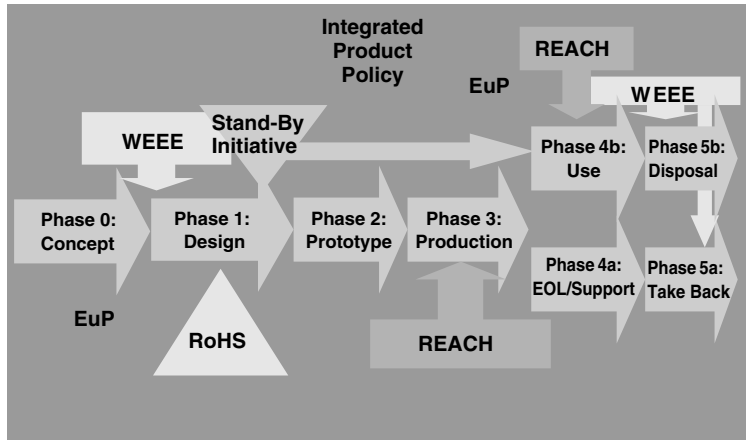


EXHIBIT 28.1 PRODUCT LIFE CYCLE VERSUS EU DIRECTIVES AND REGULATIONS

to mandating attention to potential environmental issues in the different phases of the product, and equipment, life cycle in a manner that is appropriate to the life cycle phase.[18] For example, one cannot meet EuP's requirements without specifying the requirements at the concept stage.

However, knowing and understanding Europe's environmental laws and trajectory may enable only a partial ability to comply with similar laws of other regions. Sovereign nations rarely adopt wholesale other countries' laws. While there is a modicum of consistency across many of these laws across countries and regions, the differences can be striking and, in many cases, traumatic if not planned for. Different implementation time lines and in-force dates; different reporting, disclosure, and marking requirements; inconsistent material bans; inconsistent scopes; and so on all abound in China's, California's, Japan's, and South Korea's implementation of RoHS.

In an environment like this, where inconsistent bans and requirements will continue, what is a company to do? The fundamental requirement is to understand the drivers behind, the targets of, and the trajectory for environmental regulation; then determine a strategic response that minimizes surprise.

We have reviewed the drivers, the targets, and the trajectory of product-focused environmental regulations. Next is to consider how these new types of regulations require changes to the product development process and the product life cycle itself. The first step is to organize these regulations' impacts in terms of what informational requirements result from them. An analysis of this set of environmental regulations brings four classes of attributes to be considered during product development, as shown in Exhibit 28.2.

Material Utilization Type & Amount Virgin/Recycled/Recyclable	Energy Utilization Extraction, & Processing, Use/Recovery
Life Cycle Extension	Waste Minimization Extraction & Processing, Manufacturing, Transport, Use, Recycling

Exhibit 28.2 The Four Attributes of Design for Environment

Roughly speaking, the map between regulation and attributes is:

- RoHS: material type
- WEEE: life cycle extension, waste minimization
- EuP: material type and amount, energy utilization
- REACH: material type, waste minimization

Historically, these have not been attributes that have been considered necessary in the vast majority of cases to specify in order to design, manufacture, market, or sell electronic products. In the product design and development process, for instance, the only important attributes and parameters have typically been technical ones that are functional, thermal, electrical, and mechanical in nature (and note that "functional" includes reliability—ability to function over time—as well as safety and electromagnetic interference [EMI] and similar regulatory requirements), and business ones like quality, delivery, price, and so on. Actual materials and substances themselves were only occasionally of interest (for instance, to answer questions like "how do we achieve those thermal and mechanical attributes?").

Mechanical engineers care more that a plastic they are choosing to make an enclosure from meets flammability requirements than how it achieves it. Likewise they tend to care more about the specific color and lot-to-lot consistency of that color than the particular substance or substances used to achieve that color and consistency.

The electronics industry, never a vertically integrated industry (except, perhaps, at the very beginning), has been disaggregating for decades. That pace has accelerated in the past decade with the outsourcing of actual product assembly and manufacturing, then their transfer earlier this decade to China. In outsourcing part or all of manufacturing of a product, whether it is an integrated circuit, connector, or computer, materials have been specified only when they have an

impact on a particular functional, thermal, electrical, mechanical, or business attribute. Toxicity and ecotoxicity, or waste and energy use (particularly during manufacture of the part or system), have not been attributes of concern—few or no customers had that requirement, so there was never a demand for this information. Where material is not specified, subcontractors and their supply chains have been free to choose the material, just so it meets the attributes specified.

As more and more of the ownership of material selection has been outsourced, more and more of the knowledge of what these materials actually are has also been lost upstream in the supply chain. So when material disclosures from component manufacturers are provided that include materials that could not possibly be in the part, such as solvents that volatize off in the manufacturing process (like ethylene glycol, which is a liquid with a boiling point of 198°C, which is well below the temperature the mold compound material it is part of is cured at, or alcohol called out as part of making ink), we are seeing just exactly an indication of this. And this happens frequently.

RoHS was a wake-up call to the industry that substance attributes are, in fact, important. The industry is still, to a great extent, not responding well to that call to transfer a very different type of information through the supply chain. Now, add the other attributes described earlier and you understand the magnitude of the challenge that industry faces to comply with future regulations.

28.4 A HOLISTIC APPROACH

In the previous section we identified the impact on life cycle stages and the type of impact. Understanding this type of regulation in this manner is necessary in order to identify how business and product life cycle management processes must change in order to get in front of this type of regulation, or at least ease its incorporation into today's businesses.

Exhibit 28.3 shows an example Design for Environment (DfE) planning matrix that may be considered to be an intersection of Exhibit 28.1 and Exhibit 28.2. Some examples of specific issues are indicated where life cycle stages intersect with environmental attribute targets.

A holistic approach to DfE requires that a company reconsider its entire approach to the product life cycle and modify it as needed to address environmental concerns. RoHS alone can impact every single department or organization in an electronics OEM that has anything to do with the product, so once the high-level strategy is developed, the impact to each department must be assessed, understood, and codified as changes to existing business processes or development of new ones.

Once the framework and strategy are developed, product companies should start working with their supply chains to learn what substances cannot be identified or disclosed and why not, or that might require but do not have toxicity/ecotoxicity information available for their specific application. This exercise will also identify those suppliers that are incapable of or unwilling to disclose the

		Material Type	Material Amount	Energy Use	Life Cycle Extension	Waste Streams
Product Life Cycle Phases	Concept	Target materials, resources	Target material reduction	Overall material life cycle metric	Modular design	Materials
	Design	Reusability, recyclability, hazardous material	Mass/item	DfM, design for disassembly, during component manufacturing	Upgradable	
	Prototype			Measure?		Measure?
	Production	Target reduced-energy materials: lower melting temp solders, recyclable	Fewer solder joints = less solder; serial channels = fewer wires/traces	Transportation (mass, distance): forecasting accuracy: expediting	Reusable	Wash, dross, solder, rework, energy
	EOL/Support			failure rate, transportation	Logistics	
	Take-Back	Recycling ease	Recycling value/infrastructure	Infrastructure development, preparation		Transportation
Postsale Equipment Life Cycle Phases	Use	Intentional/ unintentional release?		Total use life	Infrastructure convenience: upgrades	Effluence
	Disposal	Precautions? Scrubbing? Extra steps?	Enough volume for special recycling steps (e.g., tagging)?	Infrastructure convenience		Reuse vs. recovery vs. landfill

EXHIBIT 28.3 DESIGN FOR ENVIRONMENT PLANNING MATRIX

information. This will enable a first-order Pareto analysis of both material and supply base risk. Communicate with the suppliers that utilize suspected or known toxic substances upstream: What is their plan for authorization for REACH? What alternatives are there? What are the functional/thermal/and so on attributes of the potential replacements, and what is your time line for replacement? Understanding your supply base's approach to waste minimization, energy minimization, and material recyclability will result in more attributes that can then be used as inputs for improving product environmental performance.

Notes

1. www.panda.org/news_facts/publications/key_publications/living_planet_report/lpr04/index.cfm. A new version may well be out by the time this book is published.
2. *Energy footprint* is defined by WWF as the area required to provide or absorb waste from fossil fuels, fuel wood, nuclear energy, and hydropower.
3. Japan, however, has environmental challenges that are extremely significant as well and has also been very aggressive in addressing them. However, its footprint and approach have generally not been as externally focused or had similar external impact as the EU's. See the Japanese Ministry of Environment web page for more information: www.env.go.jp/en/.
4. http://europa.eu.int/eur-lex/en/treaties/selected/livre202.html.
5. http://ec.europa.eu/dgs/environment/index_en.htm.
6. http://ec.europa.eu/environment/newprg/strategies_en.htm.
7. Particularly European product and chemical regulations like RoHS, WEEE, EuP, ELV, and REACH.
8. http://ec.europa.eu/environment/ipp/home.htm.
9. This has not occurred without some grumbling, and even outrage. What dissent there has been, however, has been essentially from individuals rather than significant industry icons. See, for instance, www.rohsusa.com and www.cypenv.org/worldenv/files/sustainability.htm.
10. HPV substances are considered to be those put on the market in volumes over 1,000 tons per year; these substances account for over 95 percent of the chemicals on the market.
11. In the United States, the 1976-vintage Toxic Substance Control Act (TSCA), which also puts the onus on government to assess substance safety, is coming under increased scrutiny: www.latimes.com/news/nationworld/nation/la-na-toxics3aug03,1,1458223.story?ctrack=1&cset=true.
12. Specifically, the results of animal testing are to be shared between producers of the same substance, in order to reduce the number of animals required.
13. Respectively, carcinogenic category 1 or 2, mutagenic category 1 or 2, and toxic for reproduction category 1 or 2 (CMR); substances that are persistent, bioaccumulative, and toxic (PBT); and very persistent and very bioaccumulative (vPvB). See the REACH proposal for specifics at http://ec.europa.eu/enterprise/reach/index_en.htm.
14. http://usinfo.state.gov/eur/Archive/2006/Jun/09-728718.html.
15. Directive 2005/84/EC, December 14, 2005.
16. www.sfgov.org/site/uploadedfiles/bdsupvrs/ordinances06/o0120-06.pdf.

17. http://coeh.berkeley.edu/docs/news/06_wilson_policy.pdf.
18. REACH cannot be considered to be within the scope of IPP; its impact is far broader than just products. It is shown here simply because of the fact that it does impact product, including component, production, and use. It certainly may impact design as well, should chemicals be restricted, thereby forcing designs to change to replace them.

CHAPTER 29

ENVIRONMENTAL COMPLIANCE IN INDIA

Aparna Sawhney

29.1 INTRODUCTION

The institutional structure for environmental management in India began to be built systematically in the early 1970s[1] during the preparation for the 1972 Stockholm Conference on Human Development. The first pollution control legislation was enacted in 1974, and regulatory bodies were established at the center and some states. In 1976 the Constitution of India was amended to explicitly delineate the responsibility of environmental protection on the state and the citizens. In particular, the protection and improvement of forests and wildlife were made a directive principle of state policy and a fundamental duty of all citizens.[2]

Following the Bhopal gas tragedy in 1984 (due to a leak from the Union Carbide plant) a new apex body for enforcing environmental quality standards in the country, namely the Ministry of Environment and Forests, was formed in 1985. One of the most important environmental laws was enacted soon after, in 1986: the Environmental Protection Act, an umbrella legislation under which several laws and notifications have been passed since.

Today India has an elaborate set of environmental protection legislation and an intricate network of pollution control boards across the country administering these laws. More recently, the need for a comprehensive environmental management statement culminated in the National Environmental Policy of 2006, which endorsed all the different national and sectoral policies on environmental management, like the National Forest Policy of 1988, the Policy Statement on Abatement of Pollution of 1992, the National Water Policy 2002, and so on.

The polluter-pays principle has been endorsed since 1992 in India and forms the founding principle of the country's environmental policy.

The compliance of the polluter-pays principle depends on several factors, including the nature of environmental regulatory and legislative framework, the monitoring and enforcement capacity, availability and associated costs of pollution-abatement and pollution-prevention technology, and environmental awareness of the community. An environmental regime that uses market-based tools like environmental taxes/ charges and has strong monitoring capacity induces greater compliance from polluters. Moreover, greater environmental awareness and stronger preferences of the community push the industry toward greater compliance and often beyond compliance.

The environmental policy system in India is command-and-control in nature, consisting of environmental standards, mandatory installation of pollution equipment, no-objection certificates, and consents for industrial operations. The environmental standards refer both to the acceptable levels of specified parameters like particulate matter and sulfur/nitrogen oxides at industrial and residential locations (called *ambient standards*), as well as permissible levels of discharges of specified waste streams by different industrial activities (called *emission standards*). The regulatory standards are accompanied by penalties in the form of fines, imprisonment, and closure of industrial plants for errant behavior.

The monitoring and enforcement efforts of the pollution control boards across India have been more focused on *initial* or *static* compliance (i.e., installation of end-of-pipe pollution abatement equipment), rather than *continuous* or *dynamic* compliance with the emission standards from pollution points. One reason could be the simplistic assumption of the regulators that the ability to control pollution on the part of the industry would automatically lead to dynamic compliance, which does not hold as long as polluters have an incentive to avoid the operating costs of the abatement equipment. More important reasons for the deficient monitoring and enforcement system arise from institutional limitations, including inadequate monitoring infrastructure and lack of technical capacity and trained staff.

From the polluter's perspective, the incentive for dynamic compliance under the existing regime in India has been low, especially since the associated probability of detection and penalty are low. Unfortunately, an increase in monitoring does not necessarily improve compliance, as evident from a study in the mid-1990s, which found that formal inspections by pollution control board officials did not affect subsequent plant-level emissions, perhaps due to the low level of penalties imposed and the low pay of the inspectors, who were thus amenable to bribery.[3]

Regulatory factors apart, industry compliance of environmental standards can be driven by market forces, and this seems to be an emerging pattern in India. It is well known in the economic literature that firms undertake voluntary pollution prevention actions in order to project an environmentally friendly and

socially responsible market image with the goal of enhancing long-run profits. A recent event study in India assessed the effect of independent green ratings and awards by a nongovernmental organization (NGO) on the respective stock prices of firms from three polluting sectors (large automobile, paper and pulp, and chlor-alkali firms), and found that weak environmental performance is penalized in the stock market by negative abnormal returns.[4]

The Indian industry has also moved toward higher environmental benchmarking following their client specifications. This is especially true for export houses, which have acquired quality assurance and environmental management certifications, in order to maintain markets abroad. Finally, better environmental management often involves innovations to enhance resource efficiency, which leads to dynamic cost savings for firms.[5] In India, even smaller firms have begun to appreciate the benefits of increased resource efficiency and accompanying eco-profits, as illustrated in section 29.3.

29.2 CURRENT STATE OF REGULATORY COMPLIANCE AND INSTITUTIONAL CHALLENGES

The environmental standards in India are both environmental media-specific (like air and water) for residential and industrial areas, as well as industry-specific pollution norms. Industries have been divided into three color-coded categories by the Ministry of Environment and Forests based on their respective pollution potential, such as red for highly polluting, orange for moderately polluting, and green for marginally polluting. There are 17 industries under the red category, and the state pollution control boards have had special enforcement drives for the installation of pollution-treatment facilities in these industries, failing which the plants are closed down.

All three categories of industries need consent for establishment and operation under the provisions of the Water Act of 1974 and Air Act of 1981. Small-scale industries and village/cottage industries, however, need only simplified no-objection certificates from the state, while nonpolluting industrial activities like tailoring, weaving, carpentry, and the like do not require consent for operations. Moreover, since 1994 (amended in 2006) environmental impact assessment and environmental clearance have become mandatory for appraising and reviewing new projects or business expansion.

Compliance with water standards has improved partially during the past 10 years. In particular, organic pollution of aquatic resources in India, as measured in terms of biochemical oxygen demand, improved during 1994–2004, but coliform pollution remains high, especially downstream in rivers.[6] The major source of this pollution is domestic sewage from cities and towns, followed by industrial effluents.[7]

In the major cities a large part of the domestic sewage is not even collected, and the installed capacity can treat only 20 percent of the sewage generated.[8] This has led to stagnation of sewage within the cities and contamination of the

groundwater, often the only source of drinking water for the urban population. As for industrial effluents, about 60 percent of the wastewater is generated by large and medium industries, which have installed adequate treatment facilities, but the remaining 40 percent is generated by small-scale industries, most of which do not have any treatment facilities.[9]

The existing gaps in compliance with water standards have led to severe degradation in water quality in some cases. For example, the river Yamuna in North India is polluted mainly at the national capital region of Delhi, which is estimated to contribute about 79 percent of the total pollution load in the river.[10] Partially treated or completely untreated wastewater from domestic and industrial sources directly flow into the river through the city drains. Coupled with overextraction of water, the river has now lost the ability to purify itself, and has been reduced to a cesspool. More recently the regulatory attention has turned toward increasing sewage collection and treatment to improve the water quality of the river Yamuna. There is also an attempt to utilize treated water for irrigation instead of extracting more from the river, and to release fresh water into the river.[11]

The industry compliance records of the regulatory boards, particularly for highly polluting industries, are quite good. Under a program initiated in 1993–1994 for grossly polluting industries discharging into rivers and lakes, 851 industries were identified as defaulters by 1997. After these firms were served warnings, 605 firms installed treatment facilities by 2003, and the remaining 238 defaulters were closed down (mostly in the southern state of Tamil Nadu and the northern state of Uttar Pradesh). Considering the regulatory focus has been on *initial* rather than *continuous* compliance among industrial polluters, it is not surprising that water quality in rivers and lakes has not improved significantly, despite the success of this drive.

Compliance in air quality standards has also been a mixed experience. While annual concentrations of pollutants like sulfur and nitrogen oxides are largely within the national standards across India, particulate pollution remains a major problem. The monitoring data for 2003–2005 indicate that the annual average concentration of suspended particulate matter and respirable suspended particulate matter is violated in most cities.[12] Vehicles in urban India are the single largest source of respirable particulate matter, followed by industries.

The weak enforcement of environmental standards is recognized by the National Environmental Policy 2006 and is attributed to "inadequate technical capacities, monitoring infrastructure, and trained staff in enforcement institutions," the "insufficient involvement of the potentially impacted local communities," and the absence of institutionalized public-private partnerships in enhancement of the monitoring infrastructure.

While local community participation has been lacking, India has experienced a strong wave of environmental public interest litigation (PIL) prompted by individuals as well as NGOs since the mid-1980s.

Environmental PIL and the resultant judicial activism have succeeded in targeting errant firms, have ushered in new environmental regulations, and also have helped focus the regulators' attention on certain polluting sectors and industries. For instance, the remarkable improvement in urban air quality in the city of Delhi during the late 1990s directly followed from the set of Supreme Court rulings on vehicular pollution that banned leaded fuel, banned old commercial vehicles, phased out diesel-powered buses, and imposed the use of natural gas fuel.[13] Indian civil society has in its unique way supplemented the deficient formal enforcement effort and helped increase compliance in the transportation sector and among large industrial polluters.

To increase the onus on the industrial polluters, the Ministry of Environment and Forests adopted a charter on corporate environmental responsibility in 2003 for the 17 highly polluting industries. This marks the current regulatory regime's move from a narrow focus on pollution abatement toward the more holistic resource-efficiency approach. In some states, industries have been encouraged to move toward zero-discharge plants, especially in leather tanning and distilleries, through recycling and resource recovery. There are also efforts to augment the technical capacity of monitoring and enforcement by the ministry. For example, an environmental cooperation program between the Ministry of Environment and Forests and the U.S. Environmental Protection Agency in 2003 included a training of inspectors from several state pollution control entities.

29.3 CORPORATE ENVIRONMENTAL PERFORMANCE: COMPLIANCE AND BEYOND

While regulatory pressure is an important factor in environmental compliance, industrial polluters choose to improve environmental performance when it makes good business sense independent of regulatory enforcement. Indian industry has now embarked on the path of greater environmental compliance driven by economic factors: either to achieve a good market image in the case of large firms, to follow client specifications (foreign or domestic) in order to retain/expand business, or to realize cost savings with the move toward cleaner production.

The advantage of an industry movement toward cleaner production driven by economic reasons is that environmental compliance then ceases to appear as a burdensome cost (following regulation). Indeed, businesses may be encouraged to move beyond compliance and use the environmental performance of their products as a market differentiation tool to appeal to environmentally conscious consumers. This phenomenon has resulted in a plethora of voluntary product eco-labels in the industrial countries, which are used as market indicators of lower environmental impact of the concerned product, including Energy Star, Blue Angel, Greenguard, Forest Stewardship Council, and so on. A more universally accepted and popular environmental differentiator is the ISO 14001 certification for environmental management systems, which has become a popular environmental differentiator among Indian firms. The ISO 14001 represents a

more dynamic environmental compliance performance, as opposed to the *initial* compliance discussed before in section 29.1.

The ISO 14001 certifications have steadily increased in India from 400 in December 2001 to 1,698 in December 2005.[14] While the absolute number of certifications is not as impressive as those of China, Indian firms have been quick to respond to the new 2004 version, and more than half the certified firms comply with the later version.[15]

Among the larger firms in India, the adoption of better environmental practices in terms of pollution reduction, prevention, and resource saving is well documented.[16] Small firms are generally not expected to adopt environmental protection processes, as these costs are not viable for them. As noted earlier, the environmental standards for small-scale industrial units are relaxed in India and the state pollution control boards (SPCBs) at best act as facilitators for establishing common effluent treatment plants in clusters of small polluters. The SPCBs allow for some degree of nonconformity with environmental standards, since setting up of pollution control systems may not even be physically feasible given the small area of operation of micro firms.[17]

End-of-pipe pollution equipment and patented clean technology are typically too expensive for small firms, but sometimes it is possible to adopt simple pollution-preventive processes in a cost-effective manner, as has been the experience of Arjan Auto. Located in the industrial town of Gurgaon, Haryana, Arjan Auto Pvt. Ltd. is a manufacturer of automotive parts catering to the domestic market. Most of its business is conducted with Maruti Udyog Limited, the largest passenger car manufacturer in India. Although Maruti has encouraged its suppliers to adopt environmental management systems like ISO 14001, a small firm like Arjan Auto never seriously considered such a certification.[18] However, participation in a pilot project under Ecoprofit[19] succeeded in convincing the firm that it is possible to be lean and green when ecological considerations are integrated in the production process in a systematic manner.

Arjan Auto's journey with the Ecoprofit project began with the goal to reduce operational costs and improve resource efficiency of its plant.[20] Some of the measures required in the path of higher resource efficiency were very simple, like changing the layout of material flow in the factory, reusing water, and mechanical cleaning of metal parts instead of chemical cleaning for derusting.[21] Yet these simple steps raised the throughput, reduced pollution, and encouraged the company to continuously review its processes for improving its environmental and economic performance. Today the plant had undertaken two-thirds of the measures that are required for ISO environmental management system certification, and although the journey did not begin with the objective of acquiring this certification, Arjan Auto now plans to get the ISO 14001 certification next year.

This case highlights two important features: First, even when regulatory environmental enforcement is poor and the market-/client-driven incentive to adopt cleaner production is insufficient, the industry would still move toward

greater compliance if doing so raises economic profits. Second, productivity gains through better resource and environmental management can be scale-independent (i.e., can be reaped by small firms), and some measures to this end involve inexpensive plant-specific innovations.

29.4 CONCLUSION

Three decades since the establishment of the Indian environmental institution, the formal monitoring and enforcement capacity remains inadequate. However, environmental compliance has been improving despite this deficiency, aided by several factors, including informal monitoring by NGOs, judicial activism, and client demand, both domestic and foreign, for cleaner production and environmental certifications. While specific data on industrial compliance are not available, there is recorded improvement in environmental quality (air and water) in terms of some pollution parameters.

There is also a consistent increase in international certification of environmental management systems, which indicates that Indian firms are voluntarily upgrading their plants driven by economic reasons. This is true not only for large and medium firms, but for small firms, too. Contrary to the popular notion that small-scale units find adoption of cleaner processes unviable, there are cases in India where small units have voluntarily undertaken eco-friendly measures in a cost-effective manner. The example of Arjan Auto in the study highlights that the industry mind-set changes when firms are convinced that environmental planning, resource efficiency, and greater profits are complementary. Thus in spite of a lax enforcement system, firms are willing to move beyond compliance with domestic standards when it makes good business sense.

Notes

1. Although some Indian environmental legislation dates back to the previous century, the regulations prior to the 1970s were rather sporadic in nature.
2. Articles 48A and 51A(g) respectively, of the Constitution of India.
3. S. Pargal, M. Mani, and M. Huq, "Inspections and Emissions in India: Puzzling Survey Evidence," Policy Research Division, World Bank Working Paper 1810 (1997).
4. The Green Rating Project is an effort to rate industrial units within specific sectors based on their environmental performance, and was initiated by a New Delhi–based NGO, Centre for Science and Environment. Paper and pulp and chlor alkali are among the 17 industries in the "highly polluting" category of the Central Pollution Control Board. For details see Shreekant Gupta and Biswanath Goldar, "Do Stock Markets Penalize Environmentally Unfriendly Behavior: Evidence from India" *Ecological Economics* 52 (2005): 81–95.
5. M. E. Porter and C. van der Linde, "Green and Competitive: Ending the Stalemate," *Harvard Business Review* 73, no. 5 (September–October 1995): 120–134.
6. CPCB, *Annual Report 2004–05*, Central Pollution Control Board, New Delhi (2005).
7. *Annual Report 2005–06*, Ministry of Environment and Forests, New Delhi.

8. The class I and class II cities in India generate about 29,129 MLD of sewage, while the installed sewage capacity is only 6,190 MLD. CPCD, *Highlights 2005: Water Quality Assessment*, Central Pollution Control Board, New Delhi (2006).
9. This is an estimate made by the CPCB, as there is no data available. The Centre for Science and Environment, however, contends that the small-scale industrial sector's wastewater discharge may be barely 5 percent of the total (instead of 40 percent), and of this half is contributed by the small engineering sector. www.cseindia.org/programme/industry/new_images/industry.pdf.
10. CPCB, *Annual Report 2004–05*.
11. CPCB, *Highlights 2005: Water Quality Assessment*.
12. Ibid.; MOEF, *Annual Report 2005–06*, Ministry of Environment and Forests, New Delhi, 2006.
13. Prior to 1990 India had no environmental standards for vehicles, and the new rules for cleaner vehicles on city roads largely followed from Supreme Court rulings in public interest litigations to reduce urban air pollution. The first petition was filed in 1985 by the Supreme Court advocate M. C. Mehta. See Aparna Sawhney, "Managing Pollution: PIL as Indirect Market-Based Tool," *Economic and Political Weekly* 38, no. 1 (2003): 32–37.
14. Under a government financial incentive scheme to encourage ISO 9000/ISO 14001 certification among small-scale units, a one-time reimbursement of certification fees is available. www.smallindustryindia.com/schemes/eediv.htm#waste.
15. By December 2005, of the total 12,683 ISO 14001 certifications in China, only 1,385 or 11 percent corresponded to the 2004 version. By contrast, 859 of the total 1,698 certifications in India corresponded to the 2004 version. *ISO Survey 2005*.
16. For details see TERI, *Cleaner Is Cheaper: Case Studies of Corporate Environmental Excellence* (New Delhi: The Energy and Resources Institute, 2005).
17. Non-compliance in the industry has also been accepted on social grounds by the Indian regulators, most significant among them being the industry role of employment and income generation for the population at large.
18. The company, however, has other quality certifications, like ISO 9000 and automotive-specific ISO/TS16949.
19. The Ecoprofit or Ecological Project for Integrated Environmental Technology project is funded by the EU and Austria, and was introduced in Gurgaon in 2002. www.ecoprofit.org/our_members.htm.
20. Rajat Batra, director, Arjan Auto Pvt. Ltd., personal communication, October 2006.
21. The investment made by the firm under the Ecoprofit project yielded much greater savings for the firm in the medium and long terms. For some simple measures the investments were negligible but paybacks quick and high (Rajat Batra, director, Arjan Auto Pvt. Ltd., personal communication, October 2006).

CHAPTER 30

LATIN AMERICAN ENVIRONMENTAL COMPLIANCE: ENVIRONMENTAL BIOTECHNOLOGY

Hélen de Aguiar
Luiz Mário Queiroz Lima, EngD
Luiz Glück Lima
Oneglia Andrade Cavalcanti

The economic and social situation worldwide has required a new behavior from the production sector. What seemed to be correct or justifiable before is now demanding to be deeply revised. According to Lima (2001), "the new economic, social, ecological, political, and technological order presents significant changes of paradigms, which are the barriers that have to be pulled down in the Third Millennium. For this reason, topics like environment, ecology, waste treatment, etc., are not the dream of some visionaries anymore, demanding holistic solutions, implemented on a spectrum of wider amplitude, including a global view, different from previous behaviors, which mostly consisted in a focal and fragmented view;

therefore, very simple in most perspectives, in particular in the art of living in the urban environment."

Modern times require fast and precise responses to problems that put the common well-being at risk. According to Malthus' Principle, mentioned in Schneider (1994), civilized man took control of creation in such a way that the environment started to evolve, not based on the natural law any longer, but in a way that is directed to man's own benefit, to the detriment of any other species, natural balance of ecosystems, or nature's dynamic stability.

The new global order demands controlled behaviors, besides the common well-being, in scientific and technological knowledge (i.e., in intangible assets) for the balanced maintenance of relations between man and nature, as well as other beings.

This structuring movement started at Eco-Stockholm in 1972, followed by Eco-Rio in 1992, where the twenty-first-century agenda guidelines were defined. More recently, in 1996, the environmental actions were encouraged with the advent of ISO 14000 norms, which require the remediation of problems and the continuous improvement of productive processes in favor of the environment and living organisms.

At a national level, another important event motivated environmental actions: the approval of Law 9.605/98, or the Environmental Crime Law, which imposes penalties on individuals or legal entities, besides opening a discussion on the social impact of environmental management.

At a municipal level, the recently approved City Statute grants more powerful instruments of environmental control to the cities, and has been strengthened with the requirement of the Environmental Vulnerability Index (EVI), a fine-tuning instrument for the control of pollution processes in urban areas.

Based on this paradigm shift, urban waste treatment can be addressed as a fundamental theme in man's life maintenance in the biosphere, which, through the years, has been one of the greatest problems to be faced.

30.1 ENVIRONMENT AND INDUSTRIALIZATION

All industrial processes produce residues. Waste disposal caused by industrialization represents the errors of such processes, which today correspond to 30 percent of all the raw material. Many substances remaining from the industrial activities, residues of every nature, are commonly released in the environment, generating an environmental problem and consequently affecting human and animal health. Some of these compounds are generally harmful, while others are carcinogenic or mutagenic; others are teratogenic or allergenic.

Environmental pollution may occur due to natural causes, such as the contaminants emitted by volcanic eruptions; gas production resulting from marsh decomposition; or gases, such as methane and sulfidric gas, that are produced by large animals. Regarding natural pollution, the greatest environmental problems are provoked by the anthropogenic activity and its high capability to change the

raw materials in waste, particularly the harmful waste. For instance, in sulfidric acid production, for one thousand tons of sulfidric acid being produced, 20 tons of nitrogen oxide and 10 tons of sulfur dioxide are released in the atmosphere. In the metal surface treatment and galvanization area, the pollution is much higher: for each ton of treated steel, 40 tons of sludge containing heavy metals are disposed of in the environment. According to Berlyand (2000), in Europe, where clean industrialization is favored, 11 industrial nations release 9.8 million tons of sulfur in the atmosphere every year.

The greatest impact of harmful industrial waste is in the treatment and final destination of products due to technological obsolescence; every day the number of chemical products increases. According to Testa (1994), there is today in the world market around 50,000 new chemical products used by the various industrial segments. In the past five years, with the modernization of American and Japanese industries, the annual increase of one thousand new products was reported, which has diversified and made the chemical composition of industrial waste more complex.

According to Johnson (1990), the industrial waste production per capita in the United States is about 4.5 kilograms per inhabitant per day, 43 percent of which corresponds to Class I or harmful waste. Johnson also mentions that there are about 750,000 sources of dangerous industrial pollutants, 90 percent of which are receiving inadequate treatment and final disposal methods.

In Brazil, there are no statistics; there is no systemic official inference on the production of industrial waste, not even regarding harmful waste. However, studies conducted by Lima (2001) show that industrial waste production ranges from 0.3 to 0.5 kilograms per inhabitant per day, 27 percent of which can be considered harmful waste. The southern and southeastern Brazilian regions, including Minas Gerais, Rio de Janeiro, São Paulo, Paraná, and Rio Grande do Sul states, are responsible for 88 percent of the harmful industrial waste production. The northern region, particularly Pará and Maranhão states, is responsible for 2 percent of the harmful waste production, with aluminum, casting, and extraction of minerals as the greatest segments in the generation of harmful substances and Amazon degradation, particularly the soil and water resources.

The northeast region, including Bahia, Sergipe, Alagoas, Pernambuco, and Rio Grande do Norte states, is responsible for 10 percent of the harmful waste production, with oil extraction and refinement, the transport industry, as well as the petrochemical industry as the main waste producers.

(a) IMPACTS ON THE ECONOMY. Measuring the impacts of harmful waste on the economy of a country is a difficult task, as it involves a number of complex variables. However, some of these factors can be pointed out for discussion.

(i) Globalization Barriers. In spite of the resistance presented by some people, the globalization phenomenon is inexorable and irreversible, and will cause drastic changes in our lifestyles. In terms of harmful waste, the globalization

phenomenon can be translated as a commercial barrier, or sanitary barrier, once environmental quality improvements are required from industries every day, represented in ISO 14000 certifications for products and processes. The certification process enables companies to eliminate common nonconformities or anomalies in traditional industrial activity, making processes cleaner, safer, with lower product cost, and without affecting the environment and the health of workers.

Compared to other economies, Brazil still has a very low number of companies with ISO 14000 certification, which can be seen in the question of waste treatment and final destination.

In the case of Minas Gerais state, with the second largest Brazilian industrial park, the scenario is critical because, of the 107,000 companies that generate waste, only 44 of them are ISO 14000 certified—that is, comply with the international norms, do not pollute, and are prepared to export and grow.

According to *Gazeta Mercantil* (2004), Minas Gerais' economy presented in 2001 an economic dynamism lower than that of the city of Campinas, in São Paulo state. The Fundação Estadual do Meio Ambiente (FEAM) is considered responsible for the chaos instituted by the waste treatment and final destination question in Minas Gerais. The absence of technical preparation, as well as other factors, makes any licensing unavailable for at least two years, which eliminates the competitiveness of industry, increases unemployment, and aggravates the social problems in the state, such as the urban violence and reduced tax collection. It should be noted that the public sector behavior of noninvestment in agility and improvement of the licensing processes contributes to the increase of the environmental problem in the state. Such behavior is more disastrous than the industrial pollution problem, because, instead of promoting environmental protection, it promotes the anti-environmental practice. It is the moment to question, for instance, how much two years of sewage released into the environment is costing the society and the environment, while the companies have to wait for the bureaucratic licensing procedures to be concluded.

(ii) Reduction in Life Quality. The impacts on the economy caused by inadequate management of harmful waste can be measured using numerous indicators, with special attention to the reduction in life quality. The harmful waste poisons the soil, air, and water resources, making the environment unfavorable and inadequate to support life. The persistence of harmful waste in the environment creates a vicious cycle in which, at each waste disposal, there is a contamination reaction that affects and reduces the life quality, as the physical, chemical, and biological characteristics of the biosphere are irreversibly changed.

30.2 ENVIRONMENTAL BIOTECHNOLOGY ROLE

Biotechnology can contribute greatly to environmental improvement by minimizing the impacts caused by human activity on the biosphere.

This way, environmental biotechnology can operate in several segments:

- waste treatment
- sewage treatment
- decontamination—remediation of environmental problems
- reforestation and regeneration of devastated forests and biomes
- increasing the number of animal and plant species threatened by extinction.

(a) ENVIRONMENTAL BIOTECHNOLOGY APPLIED TO WASTE TREATMENT. The question of harmful waste impacts to the environment is very comprehensive, and has been a relevant subject in several countries. As mentioned by Beaulieu (1998), there are about 450,000 areas contaminated by harmful waste in the United States. According to the European Environmental Agency (EEA 1999), there are around 1,500,000 areas potentially contaminated by harmful waste in Europe, with 350,000 of them already submitted to investigation; that is, they have already been registered as areas with high potential of risk to health and the environment.

According to Liu and Lipták (2000), a study conducted in 2000 showed that the production of industrial harmful wastes in the United States reached 250 million tons. Industries of chemical products, oil, coal processing, and metal processing played a relevant role in this result.

The information on Brazilian contaminated areas is not precise. Studies conducted by Lima (2001) showed that there are about 20,000 areas contaminated by household, industrial, and hospital wastes, among others, which require remediation actions. According to these studies, the industrial activities that mostly contribute to the environmental degradation in Brazil, with the release of harmful wastes, are performed by oil companies (exploitation, refinement, and trade); oil extraction and processing; production of cement and goods; wood cutting; automotive and accessory industries; hospitals and health institutions; and municipalities. The studies also show that the household wastes, although considered Class II or noninert, present, besides foods and energy, high degrees of hazardousness, as they may contain pathogenic microorganisms, considering that most patients with pathogenic agents spend most of the healing or rehabilitation time at home, producing dangerous residues. In general, bandages, secretions, tampons, and the like are mixed with common household waste, which makes the general household waste mass a dangerous product. The greatest problem is that most of the Brazilian cities discard their waste inadequately, a fact that contributes to the creation of large waste disposal sites, which are sources of contamination, and to the increase in the number of sites requiring remediation actions.

Returning to the example of Minas Gerais, it is estimated that 20,000 tons of household waste, 7,000 tons of civil construction waste, and 107,000 tons of industrial waste are produced on a daily basis. Of the total amount, 30 percent

can be classified as dangerous due to containing substances that affect human health and the environment.

Environmental biotechnology has several tools for this waste mass treatment, with special attention to the most common solutions:

- Bioremediation
- Bioventilation
- Biofiltration
- Biobarriers
- Biolixiviation
- Phytoremediation

(b) BIOREMEDIATION. Bioremediation, one of the environmental biotechnology tools, uses decomposition of anaerobic microorganisms for waste treatment, in order to biostabilize and make wastes less soluble and therefore less impacting and dangerous.

From a commercial perspective, this technology has been applied since the end of the World War II, when the world saw industrial development and specialization. As a result, organochlorinated, petrochemical, and agrochemical solvents started being used intensively, which generated increasingly pollutant production processes and provoked the disposal in the environment of difficult-to-treat substances.

In the 1950s, there was a demand for low-cost technologies in the market that would not bring risks to the environment, in order to comply with the stringent U.S. environmental legislation. This fact encouraged the academic community to produce scientific discoveries that helped legitimize and regulate the use of the innovative technology of bioremediation.

In the 1960s, the United States, still motivated by several environmental movements, created the first laws to regulate the application and trading of bioremediation. After that, in the 1970s, there was the global milestone of this technology's acceptance by many people as an alternative for the remediation of areas destroyed by different types of waste, and large companies were created in the sector.

Finally, in the 1980s, based on progress in genetic engineering, the first patents of microorganisms were created, which motivated the bioremediation regulation as a conventional technology. This decade also reported cases of typical use of bioremediation on a large scale, such as treatment of areas affected by the oil spill from the *Exxon Valdez* in 1989, whose results were monitored by scientists and environmentalists from all over the world, confirming the efficiency of bioremediation application in large-scale environmental accidents.

Today, the market is segmented, with environmental consultancy companies and remediation work execution companies that act in damaged areas; laboratories that develop and produce microorganisms, treatment bioreactors, piles, and cells;

and laboratories for monitoring and control, as well as research and educational purposes. There are in Brazil about 190 companies that operate in this area, comprising 80 percent of the international market. The world revenue of this sector was approximately US$250 billion in 2003.

The main clients are, among others, managers of the petrochemical industry, city waste disposal sites, and industrial waste and sewage treatment. The most evident advantages offered by this technology are low operating cost, on-site treatment possibility, efficiency in the destruction of contaminants, and, mainly, the life extension of waste disposal sites, reutilization of treated areas, and segregated material recycling. The disadvantages include the absence of off-the-shelf packages and lack of knowledge by decision makers, two needs that generate the apprehension about immediate results and insecurity regarding the contracting procedures, since there will hardly be two projects with similar conditions from a geographical, chronological, and social perspective.

From the economic perspective, and considering the global scenario, the entire production process goes through an adequate and operationally and economically sustainable environmental management. In this respect, bioremediation is a great option, given its easy applicability, environmental security, and low operating cost.

Another factor that favors its application in Brazil is the tropical climate, as the country has the largest microbial biodiversity on the planet and high temperatures with small variations, if compared to temperate-climate countries. In fact, the tropical climate, combined with higher microbe activity, speeds up processes and additionally reduces the operating cost, leading us to the conclusion that bioremediation is more viable in tropical countries, in economic, environmental, and operational terms, than in temperate-climate countries.

For evaluating such effectiveness of processes, some factors should be taken into account, such as the effectiveness of inoculations and nutrient corrections, control of temperature and aerobic and/or anaerobic conditions, nondegenerative losses, waste toxicity, treatment time, material/site to be treated, and compliance with the physical schedule of the project without interruptions or discontinuities, an essential condition for bioremediation's technical effectiveness.

(c) BIOREMEDIATION OF CITY WASTE DISPOSAL SITES. The city waste disposal sites can be treated using biotechnology tools, such as bioremediation combined with cell grounding. According to Lima (2001), the residues are decomposed and biostabilized when confined in anaerobic cells, and after that, with the insertion of bovine rumen bacteria acclimatized to the site. Recombinant DNA techniques, such as the bacterial combination, are frequently used to increase the concentration of decomposition microorganisms and grant higher productivity to the treatment process. Another advantage of this technology utilization is the reuse of the same area, which extends its life and eliminates the need to find new sites for waste disposal. The operating cost of this technology for cities with

more than 100,000 inhabitants is around R$8.50 per ton of treated waste. The larger the city, the lower the operating cost.

It is necessary to question the reasons for the market structural difficulties, considering the advantages offered by this technology. First, it should be noted that bioremediation is a technology based on microbiology with application to engineering. However, such a discipline does not exist in the Brazilian academic world for the qualification of professionals in the area, so professionals who do not have a microbiology background are likely to become the decision makers. Many of these professionals are today working at organizations of environmental control in the country, being responsible for analyses and approvals of projects. In addition, most of these professionals graduated before the discovery of the bioremediation technology.

This difference in the education sector creates a great barrier for the technology, because where there is poor scientific knowledge, there is room for disinformation, myths, and prejudice, which many times lead a society to scientific moratoriums. In this context, we can point to the country's information system, which suffered numerous setbacks that generated a delay of over 20 years. Even today, with all the globalization resources, we have not been able to reach the expected development. Having policies to catch up on development is not enough; it is necessary to learn with the experience.

Another problem in the application of this technology is that in terms of bioremediation of city waste disposal sites, which is the public sector's responsibility, the projects are extremely vulnerable to political goodwill. As they are long-term projects, many times they require for their execution a longer time frame than a politician's term. If there is no administrative continuity, monitoring by the society, and effective application of the laws, such projects that have a successful history through several years are many times abandoned and replaced with obsolete and primitive technologies, which cost the public twice as much and offer gains neither to the civil society nor to the environment.

Considering how modern the theme is, it is common to have diverse institutions in the country discussing the "efficiencies of technologies" to fight environmental pollution. However, we should ask ourselves which technology, no matter its segment, will be able to resist the administrative discontinuity in the public sector and the lack of preparation of the staffing.

It could be suggested that the solution for the bioremediation consolidation in the national market does not go through interventions from this sector or another. The changes will occur with a group of measures, such as investment in specialized education; obligation of qualification courses for professionals who operate in the environmental area; creation of a database; creation of technical councils composed of experts in biotechnology in general in the environmental control organizations, qualified to provide project analysis support; and creation of mechanisms that make the market itself boost the development, application,

and monitoring of innovative technologies that are compatible with the socioeconomic, cultural, and environmental realities of the country.

Finally, it should be noted that bioremediation is globally known for its efficiency, low operating cost, and environmental security. Being a technology, it is inexorable, and it came to stay and counts on unquestionable support from the Sindicato das Empresas de Biotecnologia (SindBio, the biotechnology companies from Minas Gerais) for understanding that only access to knowledge will help change the scenario of environmental problems caused by waste disposal sites, benefiting from biotechnological tools that are now available and used successfully around the world.

(d) BIOREMEDIATION OF INDUSTRIAL WASTES. Industrial solid wastes, in particular materials resulting from processing, such as sludge, can be treated by biotechnological techniques such as bioventilation. According to Cookson (1995), bioventilation uses aerobic microorganisms and the atmospheric air as an oxygen source. In the process, the microorganisms can volatilize the organic compounds and sediment and encapsulate heavy metals. The bioventilation is largely used by the oil industry to deal with oil spills. It is also used in the treatment of organochlorinated and some refractory residues, such as PCBs (polychlorinated biphenyls), which are highly hazardous and carcinogenic. One of the techniques that should be pointed out, mainly for the treatment of residues that contain heavy metals, is biolixiviation, which is similar to the bioventilation. With biolixiviation, microorganisms are recirculated in piles of residues until the target pollutant concentration is lowered. Biolixiviation has been used in Minas Gerais successfully in the mining industry.

30.3 ENVIRONMENTAL BIOTECHNOLOGY APPLIED TO SEWAGE TREATMENT

Household and industrial sewage can be treated with biotechnology tools, mainly bioaugmentation, biobarrier, and phytoremediation.

Bioaugmentation is a technique that can significantly increase the concentration of microorganisms used in sewage treatment and still keep the perfect concentration at levels that can avoid delays in the treatment process. Another technique that has been increasingly used in recent years is the biobarrier or reactive vertical barrier, which is used in decontamination of on-site residues. The biobarriers are installed transversely to the flow or contaminant direction and colonies of decomposition microorganisms are created in these biobarriers that intercept the residues when they cross the barriers.

The use of plants combined with microorganisms, a technique known as phytoremediation, is also one of the technologies that can be used in sewage treatment and waste decontamination. The technique allows formation at the root zone of a gel composed of decomposition bacteria and fungi colonies, responsible for the mineralization or encapsulation of compounds.

30.4 ENVIRONMENTAL BIOTECHNOLOGY APPLIED TO REFORESTATION

The areas with forests destroyed or degraded by human action can be reforested with the use of vegetal biotechnology tools. The most used tool is micropropagation, consisting of the intensive production of an integral plant from the cultivation of isolated vegetal organs, tissues, and cells. One of the advantages offered by this tool, besides the fast implementation and low cost, is clone cleaning, which ensures quality and resistance to plantules and seedlings.

Another way to speed up the recomposition of native forests, in particular the ciliary woods, is the forestation in wetlands, a technology intended to accelerate the production of white woods, or wetland woods, that allows restoring integrally a wetland forest, or ciliary wood, within a period of five to seven years. The wetlands, or plain lands, are artificially built with the utilization of filter materials, sand or clay, which create a stratified profile of the soil where the plants are fixed, favoring the cycles of nitrogen, carbon, water, nutrients, and mineral salts. In the production of wetland forests, besides the presence of water throughout the entire plant life cycle, it is possible to use entophytic microorganisms that act on the biological control of plant diseases and contribute to the increase of vegetal biomass.

30.5 LEGISLATION

Federal Legislation

According to the Federal Constitution, chapter II, art. 23, the union, states, and counties must protect the environment.

Environment Universal Right

Federal Constitution, chapter VI, preservation and conservation of the environment

National Policy for the Environment

Law no. 6.938, August 31, 1981

Oil in Brazilian Waters

Law no. 5.357, November 17, 2000

Regulation no. 124 do Ministry of Interior (MINTER)

Regulation MINTER no. 124, August 20, 1980, preservation from water pollution

Industrial Activities

Edict no. 1413, August 14, 1975, preservation from industrial pollution

Health Protection

Law no. 2.312, September 3, 1954, health protection

Coast Protection

Law no. 7661, May 16, 1988, national plan for coast protection (land, air, sea)

Laws against Environmental Crimes

Law no. 9.605, February 12, 1998

Technical Standards (ABNT)

Associação Brasileira de Normas Técnicas (ABNT) published the following standards regarding solid residues and the environment:

NBR 10004—Classification
NBR 10005—Lixiviation
NBR 10006—Solubility
NBR 10007—Sampling
NBR 12988—Free liquids
NBR ISO 14001—Environment management, specification, and guidelines
NBR ISO 14004—Environment management, general guidelines, principles, systems, and supporting techniques

References

Beaulieu, M. 1998. The use of risk assessment and risk management in the revitalization of brownfields in North America: A controlled opening. *Contaminated Solid '98*.

Berlyand, M. E. 2000. *Meteorological aspects of air pollution*. Leningrad: Gidrometeoizdat.

Cookson, J. T., Jr. 1995. *Bioremediation engineering—Design and application*. New York: McGraw-Hill.

European Environmental Agency (EEA). 1999. *Environment in the European Union at the turn of the century: Facts and findings per environmental issue.* Copenhagen: European Environmental Agency.

Gazeta Mercantil (journal), São Paulo, May 15, 2004.

Horsfall, J. G. 1993. *Plant pathology: An advanced treatise*. Vol. 1. New York: Academic Press.

Johnson, K. S. 1990. *Hazardous-waste disposal in Oklahoma: A symposium*. Oklahoma Geological Survey Special Publication.

Lima, L. M. Q. 2001. *Inventário de áreas degradadas no Brasil*. Aplicações da Biotecnologia para Remediação de Lixões. Belo Horizonte. Relatório Final da LM-Tratamento de Resíduos Ltda.

Lima, L. M. Q. 2006. *Remediação de lixões municipais: Aplicações da biotecnologia*. São Paulo: Hemus.

Liu, D. H. F., and B. G. Lipták. 2000. *Hazardous waste and solid waste*. Washington, DC: Lewis Publishers.

Rifkin, J. 1999. *O século da biotecnologia—A valorização dos genes e a reconstrução do mundo*. Tradução Arão Sapiro: The Biotech Century. São Paulo: Makron Books.

Schneider, V. E. 1994. *Estudo do processo de geração de resíduos sólidos domésticos da cidade de Bento Gonçalves, RS*. Master's degree dissertation presented to Faculdade de Engenharia Civil da UNICAMP.

Shikawa, K. 1993. *Controle de qualidade total à maneira japonesa*. Rio de Janeiro: Campus.

Testa, S. M. 1994. *Geological aspects of hazardous waste management*. Washington, DC: Lewis Publishers/CRC Press, Inc.

CHAPTER 31

POLICY DEVELOPMENTS IN THE UNITED STATES RELATED TO CHEMICALS AND ELECTRONIC WASTE

Michael P. Wilson, PhD, MPH
Michael Kirschner

31.1 INTRODUCTION

This chapter focuses on policies in the United States related to industrial chemicals and electronic products and waste. For different reasons, policies in these two arenas are under considerable pressure as a consequence of developments among U.S. states and in the European Union (EU).

The first case examines the U.S. Toxic Substances Control Act (TSCA, 15 U.S.C. s/s 2601 et seq.) of 1976.[1] TSCA was an important step forward in its time and it influenced chemicals policy in countries around the world, yet its limitations have become apparent over the decades. A growing number of U.S. states are now contemplating individual chemicals policies in response to these limitations. Faced with a similar set of chemicals policy weaknesses, the European Parliament has recently approved a sweeping reform of chemicals policy known

as the Registration, Evaluation, and Authorization of Chemicals (REACH). Other nations appear to be looking to REACH as a potential model for chemicals policy, signaling that the United States is rapidly losing its status as a global leader in this arena. The importance of reforming TSCA in response to these and other developments is becoming apparent in the United States. This chapter describes the key weaknesses of TSCA, the implications of those weaknesses, and key aspects of reforms to address those weaknesses.

The second case focuses on electronic products and waste. As described in Chapter 26, electronics products contain substances, such as lead, cadmium, and mercury, that the EU has determined to be hazardous, if not in use, then as part of the waste stream. Though electronic waste currently represents a small proportion of the municipal solid waste stream (1 percent), it is the fastest growing source of solid waste in the United States.[2] Unlike the EU, the United States does not restrict the use of hazardous substances in electronic products, nor does it require electronics producers to recycle or take back electronic products at the end of their useful lives. As with chemicals policy under federal TSCA, this has given rise to state (and even city) laws and legislation pertaining to electronic waste.

These case studies suggest that, on a global scale, environmental policy is experiencing a paradigm shift driven by factors largely outside the United States, in which corporate transparency and accountability are becoming increasingly important. While leading U.S. companies have recognized that transparency and accountability are prerequisites to the triple bottom line of social, economic, and environmental sustainability, some U.S. trade associations continue to resist policy changes that would improve transparency and accountability industry-wide. As fundamental changes continue to unfold in environmental policy worldwide, it is likely that leading industries will adopt measures to improve transparency and accountability, and that these measures will include acknowledgment of public and environmental health concerns related to industry activity, along with legitimate policy proposals to address those concerns. Adopting a business-as-usual approach to global environmental policy changes, however, could lead to regulatory solutions, particularly among U.S. states, that are more costly for industry, more fragmented, less certain, and perhaps less effective in addressing root causes of public and environmental health problems. Companies would be expected to benefit from being among the first to respond to the call for reasonable transparency and accountability in emerging environmental policies.

31.2 THE U.S. TOXIC SUBSTANCE CONTROL ACT

Of all U.S. federal statutes, the Toxic Substances Control Act (TSCA) of 1976 (P.L. 94-469) is the only law that is broadly intended to enable regulation of chemicals both before and after they enter commerce. Other federal regulations that pertain to chemicals are essentially end-of-pipe statutes that do not allow review of chemicals prior to their introduction into commerce. This section describes

the overarching objectives of TSCA and describes how TSCA, in practice, has largely failed to live up to these objectives. The section concludes that a fundamental restructuring of TSCA is needed that would better meet the chemical information needs of downstream users, improve the oversight function of government, and motivate new investment in green chemistry. These changes will provide better protections for public and environmental health and will establish the market conditions that gradually favor private sector investment in green chemistry.

(a) BACKGROUND. TSCA's passage in 1976 resulted from widespread concern over the thousands of chemicals that were entering commercial and industrial use with virtually no public oversight or information on how they might affect human health and the environment. At the time, this situation was not unique to the United States; internationally, the introduction of tens of thousands of chemicals into the market preceded regulation of any kind.

Congress had three major policy objectives in enacting TSCA:[3]

1. Those who manufacture and process chemical substances and mixtures should develop adequate data with "respect to the effect of chemical substances and mixtures on health and the environment."
2. The government should have adequate authority to regulate chemical substances and mixtures that present "an unreasonable risk of injury to health or the environment, and to take action with respect to chemical substances and mixtures which are imminent hazards."
3. The government's authority over chemical substances and mixtures should be exercised "in such a manner so as not to impede unduly or create unnecessary economic barriers to technological innovation."

Prior to the passage of TSCA, the United States had no inventory of chemicals in commercial circulation, and there was no vehicle for a public agency to conduct premarket evaluation of chemicals. TSCA thus represented an important step forward in the United States in the regulation of chemicals.

(b) PROBLEMS. The size, complexity, economic importance, and rapid growth of the chemical industry have made it very difficult for countries around the world to implement effective chemicals policies. The experience of the U.S. under TSCA is no exception. Studies conducted by the National Academy of Sciences (1984),[4] the U.S. General Accounting Office (1994),[5] the Congressional Office of Technology Assessment (1995),[6] the nongovernmental organization Environmental Defense (1997),[7] the U.S. Environmental Protection Agency (EPA) (1998),[8] the U.S. Government Accountability Office (GAO) (2005),[9] former EPA officials,[10] and academic researchers[11,12] have concluded that TSCA has fallen short of its objectives. In general, all of these studies illustrate that TSCA has not provided an effective vehicle for the public, industry, or government to *assess* the hazards of chemicals in commerce or *control* those of greatest

concern. This has produced a flawed chemicals market in the United States that broadly undervalues the health and environmental effects of chemicals, relative to their function, price, and performance. As a result, TSCA has not served to motivate private sector investment in cleaner chemical technologies, such as green chemistry, and it has allowed hazardous chemicals to remain competitive in the market; this produces an array of health and environmental problems that affect the public, workers, children, ecosystems, and so forth.[13]

As described next, the weaknesses of TSCA have produced a data gap, a safety gap, and a technology gap in the United States; of these, the data gap is perhaps the most fundamental.

(i) The Data Gap. For the great majority of chemicals in commercial circulation, TSCA has provided the U.S. Environmental Protection Agency (EPA) with insufficient authority to require the *generation* of information on chemical toxicity and ecotoxicity and the *distribution* of that information to state governments, businesses, industry, and the public. In 1979, at the time TSCA was implemented, there were about 62,000 chemicals in commercial circulation in the United States—often described as "1979 existing chemicals."[14] These chemicals were grandfathered under TSCA; that is, chemical producers were not required to disclose information on their toxic and ecotoxic properties, and they were generally considered to be safe until proven otherwise by the EPA.

While TSCA assigned the EPA responsibility for assessing the risks associated with existing chemicals, it also erected barriers that have prevented the EPA from fulfilling this responsibility. In particular, before the EPA is able to require a chemical producer to generate the test data necessary for assessing risks, TSCA requires the agency to show, on a chemical-by-chemical basis, that a chemical either (1) may present an unreasonable risk to human health or the environment or (2) is produced or imported in substantial quantities *and* enters the environment in substantial quantities *or* there is or may be significant or substantial human exposure to the chemical. The EPA must also demonstrate that existing health and environmental information about the chemical is insufficient and that testing by the producer is necessary to fill the information gaps. If the EPA cannot meet these requirements, it cannot act under TSCA to require companies to generate safety information about a chemical.

This burden has created what might be called a "logical paralysis" for the EPA: To assess the public health risks of existing chemicals, the EPA needs toxicity and exposure data that producers are not required to provide—unless the EPA can first show that such a risk may in fact exist. Not surprisingly, this has turned out to be a significant barrier for the EPA. In 1994, the GAO found that the EPA had managed to review the risks of about 1,200 (2 percent) of the 62,000 1979 existing chemicals. The EPA reported to the GAO in 1994, however, that about 16,000 (26 percent) of these chemicals were potentially of concern based on their production volume and chemical design.[15]

Though the TSCA inventory has grown to 81,600 chemicals, this body of 62,000 1979 existing chemicals continues to constitute the great majority (by volume) of chemicals in commercial circulation in the United States.[16] Currently, 8,282 chemicals are produced or imported in the United States at more than 10,000 pounds per year, and 2,943 are produced or imported at more than one million pounds per year, known as high production volume (HPV) chemicals. Ninety-two percent of HPV chemicals in commercial circulation today consist of 1979 existing chemicals; only 248 (8 percent) new chemicals introduced since 1979 have reached HPV status.[17]

TSCA enables the EPA to be somewhat more active under the provisions of the statute that pertain to new chemicals introduced since 1979. These chemicals comprise 248 HPV chemicals and a number of other smaller-volume chemicals.[18] Using information submitted by producers on pre-manufacturing notices (PMNs), the EPA has acted in various ways to restrict about 3,500 (10 percent) of the 36,600 chemicals that producers proposed to introduce into commercial use between 1979 and 2004.[19]

TSCA thus enables EPA to take steps to control *new* chemicals before they are marketed; however, it only requires that producers submit toxicity testing information that is "in their possession" when they file the PMN; it does not require *new* toxicity testing, which represents a disincentive for producers to conduct toxicity testing. The EPA has reported that 85 percent of PMNs lack data on chemical health effects, and 67 percent lack health or environmental data of any kind.[20] In addition, once new chemicals are placed on the TSCA inventory, the EPA may regulate them only under the standards and burdens it carries for 1979 existing chemicals. Producers are not required to generate *tiered* health and environmental data on new chemicals as their production volume increases over time.

Finally, TSCA contains confidential business information (CBI) provisions that have prevented the EPA from *distributing* the chemical information it obtains through the PMN process and Inventory Update Rule. In 1998, the EPA reported that 65 percent of information filings submitted under TSCA were claimed by businesses as CBI. The EPA reported to the GAO in 1994 that 22 percent of these claims were invalid. In 2005, the EPA reported that 95 percent of PMNs contained some information that chemical companies claimed as confidential. State government agencies, businesses, and nongovernmental organizations have no more access to chemical information classified as CBI under TSCA than do private citizens.[21]

(ii) The Safety Gap. In addition to giving the EPA limited authority for requiring the generation and distribution of chemical information, TSCA makes it very difficult for the EPA to take regulatory action on existing chemicals and on new chemicals once they have passed through the PMN process. To regulate a chemical, TSCA requires EPA to provide "substantial evidence" that (1) the chemical

presents or will present an "unreasonable" risk to health and the environment, (2) the benefits of regulation outweigh both the costs to industry of the regulation and the lost economic and social value of the product, and (3) the EPA has chosen the least burdensome way to eliminate only the unreasonable risk. In considering regulatory actions, the EPA is required to "consider the environmental, economic, and social impact of any action" it proposes to take.[22]

Faced with this burden of proof, the EPA has been able to use its formal rule-making authority to regulate only five existing chemicals (or chemical classes) since the passage of TSCA in 1979: polychlorinated biphenyls (PCBs), chlorofluorocarbons (CFCs), dioxins, asbestos, and hexavalent chromium. Of these, TSCA itself required regulation of PCBs, and the EPA's regulation of asbestos, promulgated after the agency spent 10 years gathering evidence, was overturned in its most significant aspects by the Fifth Circuit Court of Appeals, which concluded that the EPA had failed to meet its burdens of proof required by TSCA.[23]

(iii) The Technology Gap. By not requiring producers to generate and disclose information on the toxicity and ecotoxicity of chemicals and by placing barriers to regulation by the EPA, TSCA has produced conditions in the U.S. chemicals market that have favored *existing* chemicals and have dampened industry motivation to invest in green chemistry. This has also resulted in a lack of U.S. government investment in green chemistry science, technology, and education, although practical developments in green chemistry are occurring among a number of leading U.S. chemical producers.[24] Chemistry research in the United States is lagging behind that of Japan, Italy, China, and Australia.[25] Together, these conditions may be producing a green chemistry technology gap in the United States that could have long-term implications for U.S. competitiveness in the chemicals market and for public and environmental health.

(c) IMPLICATIONS. The weaknesses of TSCA that have produced the data, safety, and technology gaps in the United States have far-reaching effects. For example, because there is a lack of comprehensive and standardized information on toxicity and ecotoxicity for most chemicals, it is very difficult for businesses and industry to identify hazardous chemicals in their supply chains or choose safer alternatives. State government agencies do not have the information they need to efficiently identify and prioritize chemical hazards. Consumers, workers, and small-business owners do not have the right kinds of information they need to identify and use safer chemical products. The lack of chemical information weakens the deterrent function of the product liability and workers' compensation systems. These weaknesses have dampened motivation on the part of U.S. chemical producers and entrepreneurs to invest in new green chemistry technologies. Meanwhile, evidence of public and environmental health concerns related to chemicals continues to accumulate.

These weaknesses have also led to a plethora of state-level actions in the United States. Many U.S. states, including California, are pursuing chemical phase outs and other policies. In 2005, for example, the California legislature deliberated on about 35 bills related to chemicals. During this same period, 18 other U.S. states considered or passed legislation pertaining to chemicals in at least five areas: brominated flame retardants (BFRs), mercury, methyl tert-butyl ether (MTBE), lead, and arsenic in wood products.[26] These state-based chemical initiatives are a natural reaction to the weaknesses of TSCA, and they reflect ongoing public concern over the health and environmental implications of chemical exposures and contamination. The number of state-based initiatives is likely to grow as the U.S. public becomes aware of the potential for double standards to emerge as REACH is implemented in the European Union.[27,28]

(d) CONCLUSION. Large sunk investments by industry in existing chemical technologies will make it difficult to transition to an industrial system based on the science and technology of green chemistry; this transition, however, will have to be made if the United States is to address a host of chemical problems affecting public and environmental health, business, industry, and government. A fundamental restructuring of TSCA will likely be needed to correct the data and safety gaps. Far more effective mechanisms will be required to improve the generation and distribution of information on chemical toxicity and to improve the ability of government to act efficiently in controlling chemical hazards of greatest concern. Correcting the data and safety gaps will enable businesses to identify and handle hazardous chemicals and to clean their supply chains of those chemicals for which safer alternatives are available. These corrections will gradually begin to shift the chemicals market such that the hazardous properties of chemicals are valued at a level comparable to chemical function, price, and performance. Companies that take full advantage of these changes could become global leaders in green chemistry innovation. Without these changes in TSCA, the current trajectory of industrial and regulatory practices in the United States will likely produce a growing set of chemically related problems for public and environmental health, businesses, industry, and government that, over time, could adversely affect the competitive position of the U.S. chemical industry.

31.3 ELECTRONIC WASTE IN ENVIRONMENTAL POLICY

To date, the U.S. government has not implemented a strategy to manage and reduce the growing stream of electronic waste. Rather, earlier this decade the U.S. EPA responded to this mounting problem by organizing a multi-stakeholder, voluntary approach, known as the National Electronic Product Stewardship Initiative (NEPSI).[29] This effort failed to produce results, however, when the U.S. electronics industry became divided over an advance recovery fee (ARF)[30] versus an extended producer responsibility (EPR) strategy. In addition to derailing

the EPA process, this division has rendered industry associations, such as the AeA (formerly American Electronics Association—www.aeanet.org) unable to establish and advocate for a clear position on federal "e-waste" policy.

U.S. states have begun to enact their own laws in response to the collapse of NEPSI. This section briefly reviews these laws and identifies the lack of harmonization among them. The products targeted, the legal requirements, and implementation strategies all differ markedly. The section proposes that this represents the worst of all possible worlds for the electronics industry, which would benefit from a single federal strategy or at least a consistent state-by-state strategy. The U.S. electronics industry, in failing to reach agreement on an ARF versus EPR approach to federal policy during the NEPSI process, may have missed a key opportunity to establish a voluntary federal e-waste standard, which could have rendered state regulations either entirely unnecessary or at least far more harmonized with federal standards.

In addition to the four active regulations discussed in this section, there are approximately two dozen other e-waste bills under consideration at present in state legislatures throughout the United States, as well as in New York City. These bills are contemplating a range of strategies to address e-waste; most, however, are adopting an EPR approach. A federal e-waste bill has also been introduced in the current (110th) legislative session of the U.S. Congress, H.R. 233.[31]

(a) FEDERAL APPROACHES. In January 2007, Representative Michael Thompson (D-CA) introduced H.R. 233, the National Computer Recycling Act. This bill, referred to the House Committee on Energy and Commerce, proposes collection of a fee not to exceed $10 for every sale of a computer or computer monitor, with substantial leeway to expand the scope to other electronic products. Besides covering administrative costs, the collected fees would be used to provide grants to people or organizations that collect, refurbish, and resell, or extract and reuse (or sell for reuse) valuable raw materials from the discarded electronic products. The bill further proposes a study to identify the types and amounts of hazardous substances in waste material from such products, and make recommendations for their end-of-life management as well as how to develop and expand the market for their reuse.

Clearly an ARF approach, this bill would address industry's desire for harmonization and minimal additional effort. However, it is likely to face resistance from states that have already invested in their own e-waste programs (and are generating revenues from those programs) and from advocates concerned that a potentially weaker federal standard could preempt more rigorous state programs.

(b) STATE APPROACHES. To date there are four states that have promulgated regulations targeting e-waste: California, Maine, Maryland, and Washington. Only one, California, has a substance restriction law focused on the use of certain substances in electronics, though other states (as well as California) have adopted

Viewable Screen Size (Measured Diagonally)	Electronic Waste Recycling Fee*
Greater than 4 inches and less than 15 inches	$6
Equal to or greater than 15 inches and less than 35 inches	$8
Equal to or greater than 35 inches	$10

*See www.ciwmb.ca.gov/Electronics/Act2003/Retailer/Fee/ for fees.

EXHIBIT 31.1 CALIFORNIA COVERED ELECTRONIC DEVICES AND FEES AT THE POINT OF PURCHASE

restrictions on the use of mercury and certain brominated flame retardants in various applications, including electronics.

(i) California. California's Electronic Waste Recycling Act (EWRA) of 2003 (SB 20/SB 50) represents an ARF approach by requiring a fee at the point of retail sale, beginning January 1, 2005, for "covered electronic devices" (CEDs). (See Exhibit 31.1.) These include:

- Cathode ray tubes (CRTs) and CRT-containing devices
- Computer monitors containing CRTs
- Laptop computers with liquid crystal display (LCD) screens
- LCD-containing desktop monitors
- Televisions containing CRTs and plasma TVs
- Plasma TVs and LCD TVs beginning July 1, 2005
- Portable DVD players beginning July 1, 2007

In all cases, the viewable screen size must be greater than four inches, measured diagonally.

Original equipment manufacturers (OEMs) of CEDs are required to notify their customers and distributors who sell products in California of their responsibilities under EWRA, which is managed by the California Integrated Waste Management Board (CIWMB).[32]

Producers must register their products with the CIWMB. The regulation allows reimbursement if the manufacturer takes back the e-waste.

The sale of CEDs in California is prohibited under EWRA if the product is prohibited from sale in the EU under the Reduction of Hazardous Substances (RoHS) directive, effective January 1, 2007, for lead, hexavalent chromium, mercury, and cadmium.[33] A separate California regulation, AB 302, effective in 2008, will ban polybrominated diphenyl ethers (PBDEs) in all applications in electronic products. AB 302 will also require disclosing the total mass of banned substances used in exempted applications in the CEDs on an annual basis. In the current California legislative session, Assembly member Lori Saldana has introduced AB 48,[34] which would expand the scope of California's EWRA to be equivalent to that of the EU RoHS directive, and track its changes. This would have the effect of tying California law to a law over which the state has no direct influence.

(ii) Maine. Maine's electronic waste law, Title 38, Section 1610,[35] lists several requirements from manufacturers of covered electronic devices. These include:

- Computer central processing unit (e.g., a personal computer)
- Cathode ray tube, cathode ray tube device, flat panel display, or similar video display device with a screen that is greater than four inches measured diagonally and that contains one or more circuit boards

CEDs in Maine do not include:

- Automobiles
- Household appliances
- Large pieces of commercial or industrial equipment, such as commercial medical equipment, that contain a cathode ray tube, cathode ray tube device, flat panel display, or similar video display device that is contained within, and is not separate from, the larger piece of equipment
- Other medical devices as defined under the Federal Food, Drug, and Cosmetic Act

Effective January 1, 2005, the law requires that a visible, permanent label clearly identifying the manufacturer be affixed to electronic products.

The law represents a shared EPR approach. Beginning in January 2006, computer monitor manufacturers are responsible for recycling costs as well as pro rata shares of orphan waste CEDs, transportation costs, and operation costs of consolidation facilities run by local governments.

Effective March 1, 2005, manufacturers are required to submit a plan for the collection and recycling or reuse of computer monitors, and as of July 1, 2007, they are required to submit annual reports to this effect.

(iii) Maryland. Maryland's e-waste law, House Bill 575,[36] effective July 1, 2006, allows counties to develop electronic waste recycling plans and establishes the Statewide Computer Recycling Pilot Program, which the state Department of the Environment's Office of Recycling will administer.

Effective January 1, 2006, manufacturers selling more than 1,000 computers in the state on an annual basis are required to pay an initial $5,000 registration fee. They must then establish a computer take-back program to recover their systems at no cost to the consumer. Manufacturers with acceptable take-back programs and appropriate labeling of their products will pay a $500 registration fee in subsequent years; companies that do not establish a recovery and recycling program or do not label their computers properly will continue to pay an annual $5,000 registration fee. In some cases, companies may find it beneficial to ignore the program and simply pay the relatively small $5,000 annual registration fee. Maryland's law represents a tax model, as compared to an ARF or EPR approach.

(iv) Washington. Washington's Electronic Product Recycling law, SB 6428,[37] represents a reasonably pure EPR model: it requires manufacturers of televisions and monitors with displays larger than four inches (measured diagonally) to provide consumer-convenient recycling of their electronic products. The law includes CRTs, flat panels, laptop computers, and desktop computers. Manufacturers of covered electronic products used by households, small governments, small businesses, and charities must make recycling services available to these groups by January 1, 2009.

Manufacturers must register with the Department of Ecology[38] and must label products with their brand name prior to January 5, 2007, after which it will be illegal to sell unbranded products in the state.

(c) CONCLUSION. While there is some commonality to the approaches adopted under these four laws, practically speaking, each one represents a different approach to the problem of electronic waste. As such, they require electronics companies that produce or sell these products to take different actions in each state. The incremental overhead required to comply with these state initiatives will place a growing burden on companies that are already struggling to maintain competitiveness in this low-margin industry sector. Whether this will drive the electronics industry nationally to craft and advocate for a single, national strategy remains to be seen.

On the present trajectory, the electronics industry could end up facing a multitude of diverse e-waste regulations across the United States, much as the U.S. chemical industry could face a plethora of state chemicals policy bills, as noted earlier. Both industries benefit from a transparent appraisal of their products' health and environmental impacts, followed by a proactive, collaborative strategy to mitigate those impacts at the federal level.

Notes

1. See www.access.gpo.gov/uscode/title15/chapter53.html—TSCA on the Web.
2. See www.epa.gov/epaoswer/osw/elec_fs.pdf—note that the EPA uses EU data here.
3. Goldman L., Preventing pollution? U.S. toxic chemicals and pesticides policies and sustainable development, *Environmental Law Review*, 32:11018-11041(2002).
4. National Academy of Sciences Commission on Life Sciences, Toxicology Testing: Strategies to Determine Needs and Priorities, Washington, D.C.: National Academy of Sciences Press, 1984.
5. United States General Accounting Office, Toxic Substances Control Act: Legislative Changes Could Make the Act More Effective (GAO/RCED-94-103), Washington, D.C.: U.S. Government Printing Office, 1994 [hereinafter GAO, 1994].
6. Congress of the United States Office of Technology Assessment, Screening and Testing of Chemicals in Commerce: Background Paper, Washington, D.C.: U.S. Government Printing Office, 1995.
7. Roe D., Pease W., Florini K., Silbergeld E., Toxic Ignorance: The Continuing Absence of Basic Health Testing for Top-Selling Chemicals in the United States (http://www

.environmentaldefense.org/pdf.cfm?ContentID=243&FileName=toxicignorance.pdf) (accessed February 12, 2005). Washington, D.C.: Environmental Defense, 1997.

8. United States Environmental Protection Agency, Office of Pollution Prevention and Toxics, Chemical Hazard Data Availability Study: What Do We Really Know About the Safety of High Production Volume Chemicals? EPA's 1998 Baseline of Hazard Information that is Readily Available to the Public (Table 6). (http://www.epa.gov/opptintr/chemtest/hazchem.htm) (Accessed May 24, 2005). Washington, D.C.: Environmental Protection Agency, 1998 [hereinafter EPA OPPT 1998].
9. United States Government Accountability Office, Chemical Regulation: Options Exist to Improve EPA's Ability to Assess Health Risks and Manage its Chemicals Review Program, p. 32. Washington, D.C.: U.S. Government Printing Office, June, 2005.
10. Goldman L., 2002, supra note.
11. Roe D., Toxic Chemical Control Policy: Three Unabsorbed Facts, ELR News and Analysis 32:10149 (February, 2002).
12. Wilson M., Chia D., B. Ehlers., Green Chemistry in California: A Framework for Leadership in Chemicals Policy and Innovation: University of California Policy Research Center (http://coeh.berkeley.edu/news/06_wilson_policy.htm) (Accessed January 16, 2007). Special Report to the California Legislature, March 2006.
13. GAO 1994, pp. 2–4, supra note.
14. National Pollution Prevention and Toxics Advisory Committee (NPPTAC) Broader Issues Work Group, How can EPA more efficiently identify potential risks and facilitate risk reduction decision for non-HPV existing chemicals?, 2005 [hereinafter NPPTAC, 2005].
15. GAO 1994, pp. 2–4, supra note.
16. NPPTAC 2005, supra note.
17. U.S. Environmental Protection Agency, The Toxic Substances Control Act (TSCA Title I), in Overview: Office of Pollution Prevention and Toxics Programs, Draft 2.0, pp. 1–23. Washington, D.C.: Environmental Protection Agency, December 24, 2003.
18. United States Government Accountability Office, Chemical Regulation: Options Exist to Improve EPA's Ability to Assess Health Risks and Manage its Chemicals Review Program, Washington, D.C.: U.S. Government Printing Office, 2005 [hereinafter GAO, 2005].
19. Ashford N., Caldart C., Technology, Law, and the Working Environment (15 USC 2605, TSCA Section 6, Regulation of Hazardous Chemical Substances and Mixtures), pp. 584–589. Washington, D.C.: Island Press, 1996.
20. GAO 1994, p. 15, supra note.
21. E. Weise, Green chemistry takes root, (http://www.usatoday.com/news/science/2004-11-21-green_x.htm) (Accessed February 9, 2006). In: *U.S.A. Today*, November 21, 2004.
22. E. Weise.
23. See the EPA Administrative Law Reporter at http://www.lawbc.com/other_pdfs/tsca.pdf.
24. See the chemAlliance.org web site: http://www.chemalliance.org/Articles/050520.asp.
25. Wilson, M., Chia, D., B. Ehlers., Green Chemistry in California: A Framework for Leadership in Chemicals Policy and Innovation, University of California Policy Research Center (http://coeh.berkeley.edu/news/06_wilson_policy.htm) (Accessed January 16, 2007). Special Report to the California Legislature, March 2006.
26. See www.ciwmb.ca.gov/Electronics/ for the home page of the law.

27. See www.dtsc.ca.gov/HazardousWaste/EWaste/index.cfm for the California Department of Toxic Substance Control's guidance on "California RoHS."
28. See http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0001-0050/ab_48_bill_20061204_introduced.pdf.
29. [1] See http://epa.gov/ecycling/links.htm and http://eerc.ra.utk.edu/clean/nepsi/ for more information.
30. The consumer pays a fee when the product is purchased; government manages recycling (California's approach).
31. See http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h233.
32. See www.ciwmb.ca.gov/Electronics/ for the home page of the law.
33. See www.dtsc.ca.gov/HazardousWaste/EWaste/index.cfm for the California Department of Toxic Substance Control's guidance on "California RoHS."
34. See http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0001-0050/ab_48_bill_20061204_introduced.pdf.
35. See http://janus.state.me.us/legis/statutes/38/title38 sec1610.html.
36. See http://janus.state.me.us/legis/statutes/38/title38 sec1610.html.
37. See the Washington State Department of Ecology Electronics home page at www.ecy.wa.gov/PROGRAMS/SWFA/eproductrecycle.
38. See www.ecy.wa.gov/programs/swfa/eproductrecycle/.

References

Ashford, N., and C. Caldart. 1996. *Technology, law, and the working environment (15 USC 2605, TSCA Section 6, Regulation of Hazardous Chemical Substances and Mixtures)*. Washington, D.C.: Island Press. 584–589.

Cone, M. 2006. U.S. rules allow the sale of products others ban: Chemical-laden goods outlawed in Europe and Japan are permitted in the American market. *Los Angeles Times*, October 8, A1, A26, A27.

Congress of the United States Office of Technology Assessment. 1995. Screening and testing of chemicals in commerce: Background paper. Washington, D.C.: U.S. Government Printing Office.

Deutsch, C. 2005. Saving the environment, one quarterly earnings report at a time. *New York Times*, November 22, 2005. http://select.nytimes.com/gst/abstract.html?res=FB0F15F9345A0C718EDDA80994DD404482, accessed February 9, 2006.

Forsberg, B. 2005a. Component compliance: Manufacturers start phasing out solder containing lead. *San Francisco Chronicle*, February 27, E-1.

Forsberg, B. 2005b. Getting the lead out: European rules force electronics companies to clean up. *San Francisco Chronicle*, January 20, C1.

Goldman, L. 2002. Preventing pollution? U.S. toxic chemicals and pesticides policies and sustainable development. *Environmental Law Review* 32: 11018–11041.

International Union of Pure and Applied Chemistry World Congress on Green Chemistry. 2001. Toward Environmentally Benign Products and Processes: Report of the Future Actions Committee (June).

National Academy of Sciences Commission on Life Sciences. 1984. *Toxicology testing: Strategies to determine needs and priorities*. Washington, D.C.: National Academy of Sciences Press.

National Pollution Prevention and Toxics Advisory Committee (NPPTAC) Broader Issues Work Group. 2005. How can EPA more efficiently identify potential risks and facilitate risk reduction decision for non-HPV existing chemicals?

Roe, D. 2002. Toxic chemical control policy: Three unabsorbed facts. *ELR News and Analysis* 32 (February): 10149.

Roe, D., W. Pease, K. Florini, and E. Silbergeld. 1997. Toxic ignorance: The continuing absence of basic health testing for top-selling chemicals in the United States. Washington, D.C.: Environmental Defense. www.environmentaldefense.org/pdf.cfm?ContentID=243&FileName=toxicignorance.pdf, accessed February 12, 2005.

United States Environmental Protection Agency. 2003. The Toxic Substances Control Act (TSCA Title I), in overview: Office of Pollution Prevention and Toxics programs, Draft 2.0. Washington, D.C.: Environmental Protection Agency (December 24). 1–23.

United States Environmental Protection Agency, Office of Pollution Prevention and Toxics. 1998. Chemical hazard data availability study: What do we really know about the safety of high production volume chemicals? EPA's 1998 baseline of hazard information that is readily available to the public (Table 6). Washington, D.C.: Environmental Protection Agency. www.epa.gov/opptintr/chemtest/hazchem.htm, accessed May 24, 2005.

United States Environmental Protection Agency, Office of Pollution Prevention and Toxics. 2005. Presidential green chemistry challenge awards program. www.epa.gov/greenchemistry/presgcc.html, accessed February 9, 2006.

United States General Accounting Office. 1994. Toxic Substances Control Act: Legislative changes could make the Act more effective (GAO/RCED-94-103). Washington, D.C.: U.S. Government Printing Office.

United States Government Accountability Office. 2005. Chemical regulation: Options exist to improve EPA's ability to assess health risks and manage its chemicals review program. Washington, D.C.: U.S. Government Printing Office (June).

Weise, E. 2004. Green chemistry takes root. *USA Today*, November 21. www.usatoday.com/news/science/2004-11-21-green_x.htm, accessed February 9, 2006.

Wilson, M., D. Chia, and B. Ehlers. 2006. Green chemistry in California: A framework for leadership in chemicals policy and innovation. University of California Policy Research Center, Special Report to the California Legislature (March). http://coeh.berkeley.edu/news/06_wilson_policy.htm, accessed January 16, 2007.

Woodhouse, E. J. 2004. Chemistry research and development: Statement of Edward J. Woodhouse, Rensselaer Polytechnic Institute. In *House Committee on Science—Congressional Testimony, March 17, 2004*. Washington, D.C.: Federal Document Clearing House.

PART 6

INDUSTRY GOVERNANCE

CHAPTER 32

ELECTRONICS GLOBAL HOMOLOGATION: REMOVING REGULATORY BARRIERS TO TRADE

Daniel P. Lawless
Shirley (Xuelian) Cui Tarantino

32.1 OVERVIEW

Homologation is the process of gaining product-level regulatory approvals. These approvals are often specific to a radio frequency (RF) technology or a telecommunications interface.

When launching any piece of electronic equipment into the global marketplace, there are a number of regulatory requirements that must be addressed. Almost

all electronic equipment must meet safety and electromagnetic compatibility (EMC) requirements, as well as environmental legislation such as Reduction of Hazardous Substances (RoHS) and Waste Electrical and Electronic Equipment (WEEE) directives. In some cases, other requirements such as import/export licenses may be required.

Radio frequency and telecom[1] products must meet additional regulatory requirements in order to be imported, marketed, sold, and/or operated in many countries around the world. Most countries have based their RF and telecom approval requirements on either U.S. or European standards. Many will accept U.S. or European test reports as sufficient proof that a product is compliant and will use this as a basis to grant approval. Other countries require product samples to be provided, in order to test the product in-country before granting approval.

32.2 HOMOLOGATION PROJECT MANAGEMENT

To launch an RF or telecom product into the global market, the manufacturer will need to obtain an appropriate set of regulatory approvals to support the target country list. This effort will typically take 12 to 16 weeks, with most countries being completed in the first 8 to 10 weeks, though the schedule can vary dramatically with new and more complex technologies.

As with most projects, proactive planning of the global homologation campaign can lead to a much smoother and more effective product launch. To get started, it is essential to understand the technologies involved, the target countries, and the product launch schedule.

In the planning stage, it is important to find the appropriate vendors to support the project. Typically a test lab and a global homologation consulting firm will be needed.

(a) VENDOR SELECTION: TEST LAB. The first stage of the project will be testing and approval for the United States, Canada, and Europe. Vendor selection at this stage is one of the most important decisions of the homologation project. A high-performing test laboratory with the appropriate accreditations and experience is a must-have when managing a mission-critical project. There are many test labs with proper accreditations, but lacking in quality and/or experience in a particular technology.

A leading-edge test lab will be able to test a product effectively against U.S., Canadian, and European standards. They will be able to explain their experience in a particular technology and commit to relevant service metrics. They will be able to provide test reports that are clear, concise, and accurate. This will lead to a more efficient process, as fewer questions will arise from the many global regulators reviewing the product application documents. Many test labs can perform testing for the United States, Canada, and Europe and have a conformity assessment body/notified body (CAB/NB) in-house, who can then issue a grant or expert opinion on the product. Additionally, some test labs have a further reach and are accredited to do testing for other countries, such as Japan, Korea, and Taiwan.

(b) VENDOR SELECTION: GLOBAL HOMOLOGATION FIRM. As the testing stage is completed, the resulting test reports will be the basis for many of the applications in other countries. At this stage, a global homologation consulting firm can help drive the approvals campaign for the product. These homologation companies have expertise in gaining regulatory approvals in many countries around the globe or in a specific region, such as Asia or Latin America. The cost and performance of these specialized companies can vary dramatically, so vendor selection will be a key task for planning an effective global campaign. Getting quotes from multiple vendors and interviewing them to get a solid understanding of their experience in the relevant technologies, as well as their service metrics, are essential. Companies with the right experience will be able to predict, with a great deal of accuracy, what the project schedule will be and which countries are most likely to be problematic.

Once vendors are lined up and cost and schedule estimates have been provided, a comprehensive project schedule can be developed, with input from all vendors. The vendors should also be able to provide accurate schedule information for most countries and identify schedule risk in countries that do not have a consistent, reliable process. Key risks to the project should be explored with the vendors and risk management plans developed as appropriate.

At this point a comprehensive homologation plan, including cost, schedule, and key risks, can be provided to the program stakeholders.

32.3 NORTH AMERICA

The U.S. Federal Communications Commission (FCC) approval can be granted either directly by the FCC or by an accredited telecommunications certification body (TCB), depending on the technology. A TCB is a private company that has obtained proper accreditations to certify certain RF products against FCC standards. In most cases, the product is first tested by an accredited test lab and a test report is generated. The test report and other product documents, such as user guides, schematics, and technical descriptions, are reviewed before an FCC grant is issued.

Industry Canada has a similar process to the FCC. A foreign certification body (FCB), a private company, is authorized to review test reports and product documentation and grant approvals, based on compliance with Industry Canada standards.

32.4 WESTERN EUROPE: R&TTE DIRECTIVE[2]

The Radio and Telecommunications Terminal Equipment (R&TTE) directive "encompasses all products using the radio frequency spectrum (e.g., car door openers, mobile communications equipment like cellular telephones, CB radios, broadcast transmitters, etc.) and all equipment attached to public telecommunications networks (e.g., ADSL modems, telephones, telephone switches)."

The directive creates a structure whereby manufacturers can test to harmonized European Union (EU) standards and self-declare that their products are compliant. In some cases where a harmonized standard is not available, a notified body can review product documentation and test reports and grant an opinion that the product is compliant with the essential requirements of the R&TTE directive. For frequencies that are not harmonized throughout EU, it is necessary to notify the appropriate authority four weeks before placing the product on the market.

32.5 REST OF THE WORLD

Once North American and European test reports have been completed, a global approval campaign can be launched. At this point, the homologation consulting firm can use the test reports and product documentation to build application binders. These binders will usually include test reports, user manual, bill of materials (BOM), schematics, operational description, photographs, and the like. Experienced consulting firms will know precisely which documents are needed for each country and will customize the application binders accordingly.

Most of these countries will grant approvals based on the information in the application binder. Some will also require a sample to be provided for in-country testing.

(a) CHINA. The largest Asian country, with the fastest growing demand for information technology and wireless products, requires testing and approval to be done in-country by government labs and agencies. EMC and safety in-country testing and approvals are required by the China Compulsory Certification (CCC). Radio frequency in-country testing and approval is required by the State Radio Regulation Committee (SRRC). Telecom in-country testing and approval is required by the Ministry of Information Industry (MII); the MII requires a local company as an applicant, and certificates are issued in the name of the local company. Factory inspection is mandatory before a CCC mark is granted.

(b) JAPAN. Radio frequency approval is issued by the Ministry of Public Management, Home Affairs, Post and Telecommunications (MPHPT) and certification agencies of the Ministry of Internal Affairs and Communication (MIC), including the Telecom Engineering Center (TELEC), which accept the testing reports from overseas mutual recognition agreement (MRA) labs and issue certificates. Japan now accepts RF certifications issued by accredited conformity assessment bodies (CABs). In some cases, a local representative may be required for RF approval. EMC registration is handled by the Voluntary Control Council for Interface (VCCI), which accepts test reports from VCCI-accredited labs. Telecom approval is issued by the Japan Approvals Institute for Telecommunications Equipment (JATE), which accepts reports from overseas labs. Most electrical appliances for home and business in Japan are subject to the Electrical Appliance and Material

Safety Law (DENAN Law), which requires the Product Safety Electric Appliance and Materials, or PSE-mark.

(c) SOUTH KOREA. Radio frequency and telecom approvals and EMC certification for Information Technology Equipment (ITE) are issued by the Radio Research Laboratory (RRL), which is organized under the Ministry of Information and Communications (MIC). The RRL accepts EMC, RF, and telecom test reports from overseas labs accredited under the MRAs. Safety approval for the Korea EK mark is basically equivalent to EU standards except for some national variations. The EK mark requires testing in-country or by MRAs. A local representative is required for all Korea approvals. Factory inspection is required for the EK mark.

(d) TAIWAN. Radio frequency and telecom approvals are issued by the National Communications Commission (NCC). The NCC accepts RF reports from overseas labs accredited under the MRA. A local representative is required. Telecom approval requires in-country testing by the NCC. EMC and safety approvals are issued by the Bureau of Standards, Metrology, and Inspection (BSMI), which accepts EMC reports from overseas accredited labs. The Certification Body (CB) scheme[3] is not recognized in Taiwan. Safety testing must be done in a local lab. NCC approval for RF, telecom, and BSMI are issued in the name of the local representative.

(e) INDIA. Radio frequency approvals are issued by the Wireless Planning and Co-ordination Wing (WPC) and are based on Conformité Européene or European Conformity (FCC/CE) test reports. A local representative is not necessary. Telecom approvals are issued by the Telecommunications Engineering Center (TEC), which is organized under the Department of Telecommunications (DoT). For telecom equipment, FCC/CE reports are accepted in addition to mandatory in-country testing against TEC standards. Local representation is required.

(f) INDONESIA. Radio frequency and telecom approvals are issued by the Directorate General of Posts and Telecommunications (DG PosTel). FCC/CE reports are accepted, in addition to mandatory in-country testing. Local representation is required.

(g) MALAYSIA. RF and telecom approvals are issued by the Standards and Industrial Research Institute of Malaysia (SIRIM). RF approval is based on FCC/CE reports and a physical sample must be submitted to the SIRIM in person. Telecom equipment does require in-country testing. Each local distributor that will import the product must have approvals issued in its name.

(h) PHILIPPINES. RF and telecom approvals are issued by the National Telecommunications Commission (NTC). RF approval is based on FCC/CE reports. A local representative needs to submit the application documents to the NTC. Telecom approval requires in-country testing with local carriers.

(i) SINGAPORE. RF and telecom approvals are issued by the Info-Communications Development Authority (iDA). RF approval is based on FCC/CE test reports and certificates. Certificates are issued in the name of local companies with dealer licenses. Telecom approval requires testing by an iDA-certified lab.

(j) HONG KONG. RF and telecom approvals are issued by the Office of the Telecommunications Authority (OFTA). RF approval is based on FCC/CE test reports and certificates under a volunteer approval process. Certificates can be issued in the name of manufacturer or local authorized dealer. Telecom approvals require testing by an OFTA-certified lab.

(k) THAILAND. Telecom approvals are issued by the Telephone Organization of Thailand (TOT) to the local carrier. The National Telecommunications Commission (NTC) is in the process of certifying local carriers. The NTC accepts FCC/CE reports, and currently RF approvals are not required in Thailand instead of an import permit.

(l) VIETNAM. RF and telecom approvals are issued by the Directorate General of Posts and Telecommunications (DGPT). RF and telecom devices must meet the technical and operational conditions prescribed by the DGPT. FCC/CE reports are recognized. Each local distributor that will import the product must have approvals issued in its name.

(m) MEXICO. RF and telecom approvals are issued by the Comisión Federal de Telecomunicaciones (COFETEL) or Federal Telecommunications Commission. FCC/CE reports are accepted. The Normas Oficiales Mexicanas (NOM) or Mexican Official Standards product safety approval is also required for certain products. A local distributor is required, and each importer/local dealer must have approval issued in its name.

(n) BRAZIL. RF and telecom testing can be done by accredited private labs, designated by the Agencia Nacional de Telecomunicacoes (ANATEL) or National Agency of Telecommunications. Applications are issued by the Designated Certification Organization (OCD), then reviewed and approved by ANATEL. Product safety approvals are required by the Instituto Nacional de Metrologia, Normalizaçã̃o e Qualidade Industria (INMETRO) or National Institute for Standardization and Industrial Quality. Local representation is required.

(o) ARGENTINA. RF and telecom approvals are issued by the Comisión Nacional de Comunicaciones (CNC) or National Communications Commission. FCC/CE reports are accepted, in addition to mandatory in-country testing. Product safety approvals are required by the Direccion Nacional de Comercio Interior (DNCI) or National Office of Internal Commerce. Local representation is required.

(p) CHILE. RF and telecom approvals are issued by the Subsecretaría de Telecomunicaciones (SUBTEL) or Ministry of Transports and Telecommunications. Product safety approval is required by the Ministry of Economy, Development and Reconstruction, which is controlled by the Superintendence of Electricity and Combustion (SEC). Chile has changed regulation twice in recent years. Currently Chile accepts FCC reports of RF products. Telecom approval requires in-country testing done by an accredited lab. Local representation is required.

(q) VENEZUELA. RF and telecom approvals are required by the Consejo Nacional de Telecomunicaciónes (CONATEL) or National Commission of Telecommunications. Venezuela accepts FCC reports and is considering a formal approval process similar to FCC as its national radio law. Local representation is required.

(r) COLOMBIA AND ECUADOR. In Colombia, RF approval is issued by the Comisión de Regulación de Telecomunicaciones (CRT) or Commission of Telecommunications Regulation. In Ecuador, approval is issued by the Secretaría Nacional de Telecomunicaciones (SENATEL) or National Secretariat of Telecommunications. Both countries require FCC reports to import the product. Local representation is not required. An end user may be required to register outdoor systems with the local government office.

(s) AUSTRALIA AND NEW ZEALAND. Australia and New Zealand have a mutual recognition agreement (MRA) with the EU, and RF, telecom, safety, and EMC standards are adapted from CE requirements. Testing must be done in an Australia Communications and Media Authority (ACMA)-accredited lab. For RF and telecom products, Australia and New Zealand do not require national certification, but rely on a self-declaration process. A local representative is required to hold the compliance folder. The local representative must be registered with the ACMA and have a supplier code.

(t) SOUTH AFRICA. RF and telecom approvals are required by the Independent Communications Authority of South Africa (ICASA). CE reports are accepted and in-country testing is required for some products. Local representative is required.

(u) RUSSIA. RF and telecom approvals are required by Gosstandart of Russia (GOST-R), the State Committee of the Russian Federation for Standardization and Metrology. Gosstandart of Russia is the national certification body of the Russian Federation and is responsible for issuing the certification and enforcing the certification system.

(v) TURKEY. RF and telecom approvals are required by the Telecommunication Authority of Turkey (TA). Turkey accepts CE reports for RF products. Telecom devices are required in country testing. Turkey has adopted the R&TTE directive.

(w) ISRAEL. RF and telecom approvals are required by the Ministry of Industry, Trade, and Labor (MoIT). Israel accepts CE reports. Israel requires samples in some cases. Tests are often conducted at the Standards Institute of Israel, which issues the approval.

(x) SAUDI ARABIA. RF and telecom approvals are required by the Communication and Information Technology Commission (CITC). Saudi Arabia accepts CE reports for RF products. Telecom devices require in-country testing. The approval can be issued to the importer or the manufacturer.

32.6 PRODUCT COLLATERAL

Once a product is approved, country-specific requirements for product collateral must be addressed. Many countries have labeling requirements that indicate that a product has been approved by the appropriate authority or designated assessment body. User guide statements are sometimes mandatory, and there may be specific local language requirements. After these issues have been addressed, in most cases, the product can be imported, marketed, operated, and sold.

32.7 THE FUTURE: POSITIVE REGULATORY TRENDS

There are a number of positive trends within the global regulatory arena, which are creating better efficiency for manufacturers and removing regulatory barriers to trade.

The R&TTE directive (1999/5/EC) was a great step forward in Western Europe. Manufacturers now have multiple options for CE marking products and demonstrating compliance with regulatory standards. For example, they now can test RF products against harmonized standards and self-declare compliance against essential requirements of the directive. This process has removed national approval schemes and the need for regulators to grant individual product-level approvals. Within the directive, there are also provisions for dealing with technologies that are not covered by current harmonized standards. Notified bodies are private companies that have an appropriate accreditation to review products and grant opinions as to whether a product is in compliance with the essential requirements of the R&TTE directive.

There are a number of mutual recognition agreements (MRAs), which are further improving the homologation process. The U.S.-European Union MRA allows European notified bodies and U.S. conformity assessment bodies (CABs) to assess products and provide expert opinions and/or issue grants for both the United States and Europe. This allows greater efficiency for manufacturers, which can now address both North American and European approvals through one company.

In the Asia-Pacific region, the Asia-Pacific Economic Cooperation Telecommunications Information (APEC TEL) MRA is progressing, and we are now seeing recognition of foreign test labs and accreditation of private certification

bodies or CABs. This allows the manufacturer to obtain regulatory approvals while testing in fewer places and to gain certificates from fewer organizations. This is a currently evolving process, and positive steps forward are now being realized in several Asia-Pacific economies.

Notes

1. There are many RF and telecom technologies, and regulatory requirements vary dramatically for each country. Within the RF technologies, there are both licensed and unlicensed devices with varying requirements. For this discussion, WLAN is used as an example technology for RF and an analog modem is used as an example for a telecom product.
2. The Directive 1999/5/EC: http://ec.europa.eu/enterprise/rtte/index_en.htm.
3. The CB scheme is based on the mutual recognition principle by using internationally accepted certification standards. The CB scheme virtually eliminates duplicate testing and facilitates the global sharing and acceptance of product safety results across participating laboratories, also called national certification bodies (NCBs). The CB framework is established by the International Electrotechnical Commission (IEC) as a means to reduce barriers to cross-border trade for various types of electrical and electronic equipment.

References

APEC Telecommunications MRA—Exporter's Guide. www.mac.doc.gov/tcc/e-guides/eg_apect.html.

APEC Telecommunications MRA—Working Group. www.apectelwg.org/.

European Commission—R&TTE Directive. http://ec.europa.eu/enterprise/rtte/index_en.htm.

FCC Equipment Authorization. www.fcc.gov/oet/ea/.

NIST CAB MRA US-EU. http://ts.nist.gov/Standards/Global/mra-eu-telecom.cfm.

US EU MRA. www.mac.doc.gov/mra/mra.htm.

CHAPTER 33

PROTECTING THE INNOCENT: THE INFORMATION SECURITY AND PRIVACY BATTLE

Lane Leskela

33.1 RECENT HISTORY OF PRIVACY REGULATIONS IN THE UNITED STATES

The May 2006 revelation that the U.S. National Security Agency had been searching a database of millions of telephone records and mining it for potentially threatening patterns is just one of the latest in a long series of conflicts between individual privacy and the increasing ability to manage mass quantities of data involving individuals. These conflicts will increase and challenge the ability to enforce civil rights in the United States and other countries even in the presence of more stringent legal protections.

In the regulatory domain, the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), set a benchmark for the protection of consumers' personal information held by financial institutions in the United States. GLBA requires "appropriate standards for ... administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized

access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

The GLBA privacy requirements cover three areas: the Financial Privacy Rule, Safeguards Rule, and "pretexting" provisions. GLBA gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to financial institutions, which include not only banks, securities firms, and insurance companies, but also companies lending, brokering, or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, and collecting consumer debts. The U.S. Federal Trade Commission regulates these other nontraditional financial institutions.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, that receive this information. The Safeguards Rule requires financial institutions to design, implement, and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions. The pretexting provisions of GLBA protect customers from individuals and companies that receive their personal financial information under false pretenses (the practice known as pretexting).

In October 2001, in response to the attacks on the World Trade Center in New York on September 11 of that year, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) introduced a wide range of legislative changes to increase the surveillance and investigative powers of law enforcement agencies in the United States. The USA PATRIOT Act introduced amendments to the Wiretap Statute (Title III), the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the Foreign Intelligence Surveillance Act, the Immigration and Nationality Act, the Family Education Rights and Privacy Act, the Pen Register and Trap and Trace Statute, the Money Laundering Act, the Money Laundering Control Act, the Bank Secrecy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act. The USA PATRIOT Act expanded government investigative authority, especially with respect to the Internet. These provisions implicate constitutional protections of individual liberty, including the procedures for interception of information transmitted over the Internet and wireless services.

In 2003, the California state legislature went a step further with regard to the protection of personal information in Senate Bill 1386. This law requires California's state agencies, individuals, and businesses that are licensed to conduct business in California managing "computerized data that includes personal

information" to disclose "*any* breach of the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

33.2 PERSONAL DATA PRIVACY PROTECTION IN EUROPE

The European Union Directive on Data Protection of 1995 specified that each member nation pass a national privacy law and create a personal data protection authority to protect their citizens' information privacy and to investigate any privacy breaches. After more than a decade, national privacy laws in Europe still vary somewhat, given the persistence of different local customs and traditions. As a whole, however, privacy laws in Europe reinforce a basic principle: privacy is a human right. With this tenet, European privacy law is far more consistent than data privacy protection in the United States. For example, in the European Union:

- Personal information cannot be collected without consumers' permission.
- Individuals have the right to review all collected data and correct any inaccuracies.
- Companies that process personal data must report their activities to the national government's data protection authority.
- Employers cannot read their workers' private e-mail.
- Personal information cannot be shared by companies, or across national borders, without express permission from the individual.
- Checkout clerks cannot ask for shoppers' home phone numbers.

Interestingly, while companies face detailed regulations limiting their use of European consumers' personal information, European governments are generally exempt from such limitations. Whereas the open use of individual credit reports is comparatively rare in Europe, wiretapping is common. In the Netherlands, for example, there were 130 times more wiretaps than in the United States in a recent year. Most Western Europeans carry some kind of national identification card, whereas the U.S. Social Security card is not issued for that purpose and general use of an individual's Social Security number is highly restricted. In Germany, citizens and long-term visitors must register and update their current addresses with local police—a practice that is also common in many countries outside of Europe, and most particularly in Asia.

The reason that privacy laws in Europe and the United States are quite different is due to long-held cultural beliefs: Europeans generally distrust corporations more than Americans, and Americans are typically more suspicious of government and fear government invasions of privacy. As a result, U.S. federal agencies have been granted far less power to limit the potentially privacy-invading activities of private companies. The Federal Trade Commission (FTC), the agency charged with protecting U.S. citizens from personal data privacy violations, rarely acts directly against U.S. companies. When the FTC does act in such matters,

its solutions are generally restricted to small fines and overwhelmingly result in out-of-court settlements.

Countries in the European Union, however, use their respective personal data protection authorities to proactively monitor corporate requests for and dissemination of individual information. European consumers can appeal directly to their nations' data protection authorities, which, in some countries (France and Italy represent outstanding examples) have extensive subpoena power. Corporate fines for personal data privacy breaches in these countries are common.

33.3 CRITICAL ROLE OF ACCOUNTABILITY IN INFORMATION SECURITY

According to Steve Schuster, director of IT security at Cornell University, from February 2005 to July 2006, the data of U.S. citizens contained in over 89 million records were at risk of nonauthorized disclosure. In addition, of 237 reported data breaches during this period, 83 took place in institutions of higher education. The ongoing debate regarding information security (access vs. privacy) is often miscast as a zero-sum game: Increased information security can be achieved only by giving up some of the elements associated with the individual's right to privacy. But the reality is that sacrificing privacy does not necessarily result in greater security, and greater security does not necessarily require an erosion of privacy.

Information technology has bolstered the investigatory confidence of many organizations required to respect the legal controls of probable cause and due process. Information technology advances also challenge individual privacy by making terabytes of personal information inexpensive and easy to store, search, and retrieve. But with well-documented and widely deployed security solutions in place, why is protecting sensitive data still so difficult? Why are security breaches fairly common? The wide assortment of technical solutions includes network firewalls, personal firewalls, operating system patches, antivirus and anti-spyware software, data encryption, intrusion-detection and intrusion-prevention systems, and embedded security management systems. The most sensitive data can and should be safeguarded through the deliberate combination of these proven applications.

The flaws in data privacy management are not due to technical security capabilities but rather to inadequate personal accountability for data protection and inconsistent practices. The weakest security link in any organization is its people. Data protection ultimately hinges on personal responsibility for the ways in which computers are used and careful handling of the data that individuals are responsible for. Consistent cultural alignment within organizations reinforced by conscientious personal behavior will reduce growing security threats, the risks to organizational reputation, and heightened security legislation.

Poor data-handling procedures (local drive storage of copies of spreadsheets that contain Social Security numbers, as opposed to deleting all copies or moving

an encrypted single copy to external storage) put personal data at risk. We must be made aware of the sensitivity of data within our control and be made personally responsible for the consequences of risk to which this data is exposed. We need to clearly understand which data require specific levels of increased protection, where specific data must be transmitted and stored, and who has authorized access to retrieval and dissemination. According to IT security director Schuster, enforcing data management requirements such as operating system patch levels, password complexity standards, designated antivirus solutions, and access control procedures can address about 90 percent of security challenges.

The following is a recommended (but not exhaustive) set of best practices for data protection for sensitive information:

- Identify and remove all unencrypted copies of unnecessary files—typically spreadsheets and documents—that contain Social Security numbers, credit card numbers, driver's license numbers, and account numbers.
- Establish random password conventions on all user accounts and a policy of frequent password changes (at least every month).
- Identify and strip unknown and suspect file formats from incoming e-mail at the firewall.
- Run antivirus software with a minimum of daily virus definition updates.
- Restrict access to an individual computer by an assigned employee or staff member. Eliminate file-sharing options or configure file sharing with strong password requirements.
- Shut down or enforce automatic log-off of a computer after a maximum of 30 minutes of inactivity.
- Regularly screen for and eliminate spyware.

To take the necessary steps to better protect personal and private data within any organization, the following questions must be answered:

- What defines the data that the organization must protect?
- Is the requirement for data protection the result of regulation, civil liability, business relationships, or any combination of the three?
- Where is private data gathered and used within the organization?
- What are the fundamental criteria for access to and use of private data?
- Are documented processes in place to grant and remove access to private data?
- Is access to private data sufficiently controlled, based on priorities for the risk of exposure?
- Are policies in place to ensure that access to this data is not being abused?
- Are specific punishments (legal and otherwise) in place for the individual breach and abuse of private data?
- Are approved processes in place to assess, audit, and reprioritize risks to private data?

- Who is individually responsible for the security and protection of each category or domain of private data?
- Are processes in place to identify and quickly and completely respond to compromised data?

33.4 FOR FURTHER CONSIDERATION—INDIVIDUAL RECOGNITION TECHNOLOGY

The shift from analog to digital data format is the single most challenging—and, from the surveillance perspective, potentially rewarding—transformation in security technology. With analog video cameras, someone needed to watch the video feed for an individual's privacy to be compromised. It was expensive to catalog and store videotapes, and time-consuming to find relevant portions after the fact. This was the purview of law enforcement with warrants for wiretapping, racketeering, mail fraud, and similarly suspect criminal activity. With the advent of digital video cameras, it has become inexpensive to store and retrieve live images. Investigators or private individuals can search video files by tagging the precise points where someone is moving in the frame.

Facial-recognition software is now advancing at such a rate that, given the quality of still and moving images in video format, a single individual will be quickly identified whenever he or she was in front of a camera. Moreover, digital data fraud in the form of image retouch, transformation, and replacement software is now available on the desktop. Any individual with a digital video file can be made to appear performing virtually any act in any location at any time. Thus the technology battle has shifted to frame encoding to identify original sources, back to the equipment used to capture initial images.

Practical difficulties and expense used to be the main obstacles to invasions of privacy. The openness of personal data once held in complex proprietary databases has focused attention on the gray areas of third-party information management across legal jurisdictions. At the same time, with the global sharing of individual information databases, the ability to track suspects across Interpol, FBI, CIA, and Scotland Yard resources is nearing the point where it is as timely and accurate a process as identifying a judge leaving a brothel in Canada or a security officer making the rounds between bank branches in Hong Kong.

References

Granick, Jennifer. 2006. Security vs. privacy: The rematch. *Wired News*, May 24.

Proposed rules. 2000. *Federal Register* 65, no. 174 (September 7).

Schuster, Steve. 2006. Why can't we protect our data? *Educause Review* 41, no. 5 (September/October).

Sullivan, Bob. 2006. "La difference" is stark in EU, U.S. privacy laws. MSNBC, October 19.

CHAPTER 34

SHIPPERS COMPLIANCE IN FREIGHT TRANSPORTATION AND LOGISTICS

David Jacoby

34.1 INTRODUCTION

Rules and regulations in the transportation and logistics field may be grouped into two categories: (1) regulation that affects carriers (transportation and logistics companies providing freight movement services) and (2) regulation that affects shippers (companies that hire others to move freight). The government imposes many regulations on carriers that shippers may be unaware of. Conversely, many shippers are unaware of the regulations imposed on the carriers that they hire.

This chapter highlights significant regulations faced by shippers—companies hiring other companies to move freight—and a separate one (Chapter 40) focuses on regulations affecting carriers. Both provide an overview of the bodies of law affecting each group so both shippers and carriers may have an appreciation for the regulatory environment affecting each other, as well as a familiarity with the most common laws that could affect their businesses.

Shippers must comply with government-imposed import and export regulations. They must also be sure to properly declare and classify any hazardous materials to conform to the law. But shipper compliance extends beyond these legal obligations, since trading partners expect shippers to comply with a number of generally accepted financial and commercial protocols such as incoterms (international commercial terms) and letter of credit formats, and customers will expect them to comply with their proprietary delivery, packaging, and information submittal standards.

This chapter uses the United States as a reference point for defining compliance issues. Because of the legislative nature of compliance issues, the institutional and regulatory framework is different outside of the United States.

34.2 KEY REGULATORY BODIES

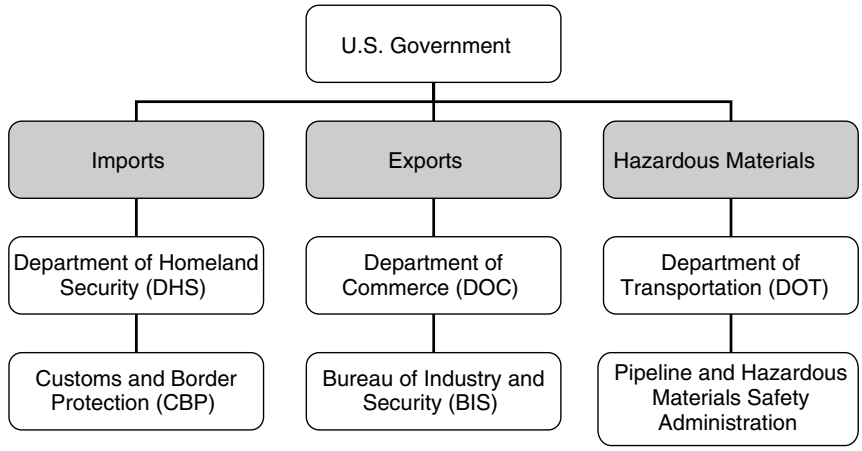
In the United States, three agencies define the compliance requirements for shippers:[1]

1. The Department of Homeland Security (DHS)'s Customs and Border Protection (CBP) division enforces customs rules at the borders, has the final say on classification of imports, and administers programs such as the Customs Trade Partnership Against Terrorism (CT/PAT).
2. The Department of Commerce (DOC)'s Bureau of Industry and Security (BIS) publishes a set of lists of prohibitions and requirements.
3. The Department of Transportation (DOT)'s Pipeline and Hazardous Materials Safety Administration regulates what can and cannot be traded, and specifies rules for safe signage, storage and handling, and so on.

These agencies, which have jurisdiction over imports, exports, and hazardous materials, respectively, are shown in Exhibit 34.1.

In addition to specific import, export, and hazardous materials laws, two important laws that apply to international commerce with the United States:

1. The Foreign Corrupt Practices Act, enacted in 1977 and enforced by the Department of Justice, forbids bribes or gifts of any kind to foreign businesses or governments. The law requires companies to implement responsible internal accounting controls, keep records, and refrain from bribing foreign officials.
2. Anti-boycott laws, enacted in the 1970s and enforced by the Bureau of Industry and Security, prohibit Americans from participating in another nation's boycotts or embargoes. These laws were specifically designed to limit pressure from non-American interests against their American customers or suppliers to boycott commerce with strategic allies (e.g., Israel) as a protest against U.S. foreign policy.



Source: Boston Logistics Group.

EXHIBIT 34.1 U.S. GOVERNMENT AGENCIES DIRECTLY AFFECTING SHIPPER COMPLIANCE

34.3 IMPORT REQUIREMENTS

(a) PROHIBITED ITEMS. Customs and Border Protection (CBP) prohibits selected categories of items in whole or in part from importation. These include:

- Absinthe.
- Automobiles (they must meet U.S. emissions standards).
- Biologicals (they need a permit from the U.S. Department of Agriculture).
- Cultural artifacts and cultural property (they require documentation to ensure that their export does not violate country of origin rules).
- Dog and cat fur.
- Drug paraphernalia.
- Firearms (these must go through a licensed importer, dealer, or manufacturer).
- Fish and wildlife (to protect endangered species).
- Fruits and vegetables (they are subject to review by the U.S. Food and Drug Administration).
- Game and hunting trophies (these must pass through a designated port of entry and may be subject to inspection).
- Gold (if being imported from Cuba, Iran, Iraq, Libya, Serbia, or Sudan).
- Meats, livestock, and poultry, and prepared food products that include meat (to avoid contamination and disease).
- Medication (primarily to control narcotics and similar abusive substances).

- Pets (subject to approval based on age and physical condition, in order to prevent the spread of disease).
- Soil, plants, and seeds (subject to conditions that vary over time, to prevent the spread of disease).
- Trademarked and copyrighted articles.

(b) IMPORT DUTIES. The level of import duty is specified in tariffs. U.S. tariffs are relatively low—the average ad valorem rate is 4.5 percent[2]—but filing proper customs documentation can be complex. Over 27,000 categories of items are taxed on import, and there are over 13,000 categories of taxes,[3] meaning that about half of the duty categories are specific to narrow categories or even individual items. Failure to account for duties completely and properly can result in significant penalties and fines. Shippers must keep all customs documents for a minimum of five years after the transaction closes, per the Customs Modernization Act of 1993, and shippers are liable for errors in documentation.

(c) VALUATION. While importers may wish to reduce their tax liability, under-invoicing to reduce import duties is subject to fines.

The General Agreement on Tariffs and Trade (GATT) Valuation Code, which the United States adopted in 1980 and which most of its trading partners use, stipulates transaction value as the predominant basis for valuing imported materials. Where transaction is not between third parties, for example between two subsidiaries inside a company, the shipper can approximate market value by using comparable bases such as the transaction value of similar merchandise, computed value (a cost buildup), or deductive value (based on additions and subtractions from a reference price).

In determining value, the cost of materials, packaging, and selling commissions, royalties, or license fees incurred by the buyer may be included. However, the cost of transportation, insurance, shipping, and logistics services, including assembly after importation, as well as customs duties and other federal taxes, are excluded from the valuation basis.

(d) IMPORT DOCUMENTATION. Common import documents include:[4]

- Bill of lading, airway bill, or carrier's certificate (naming the consignee for customs purposes) as evidence of the consignee's right to make entry
- Commercial invoice obtained from the seller, which shows the value and description of the merchandise
- Entry manifest (Customs Form 7533) or entry/immediate delivery (Customs Form 3461)
- Packing lists, if appropriate, and other documents necessary to determine whether the merchandise may be admitted

Standards for the accuracy and completeness have increased in recent years due to security concerns. The clear identification of the consignee is required,[5] and CBP no longer permits generic descriptions such as "FAK" for "freight all kinds."

Shippers must provide all data to carriers long enough in advance to allow the carriers to meet advance manifest declaration requirements. Carriers shipping air or sea freight to the United States must file all papers 24 hours prior to scheduled departure, per the 24-hour rule. Truck shippers must have customs data processed a minimum of one hour before the shipment arrives at the border, as stipulated by CBP in its Final Rule on the Trade Act of 2002.[6]

(e) VOLUNTARY PROGRAMS: CT/PAT AND OTHERS. The U.S. government and shipper community developed a voluntary set of guidelines after 9/11 (the Customs Trade Partnership Against Terrorism, or CT/PAT) that help identify and speed cargo through customs for low-risk shippers whose supply chain processes have been validated as safe and secure. Customer screening, recognized by CT/PAT as a best practice, encourages shippers to know their customers and the end use of their products in order to be able to identify a suspicious use of equipment or technology for a potential terrorist attack. For example, a bakery ordering a supercomputer or a customer in a country that uses 220 volts ordering a system based on a 120-volt standard would trigger an inquiry. In such cases, the exporter has a duty to inquire about end use and destination, and if it is not satisfied with the response, it must report the situation to the Bureau of Industry and Security (BIS).

34.4 EXPORT REQUIREMENTS

(a) PROHIBITIONS. The U.S. Bureau of Industry and Security requires an export license for shipments to certain embargoed countries. At the time of writing (2007), this list includes Iran, Iraq, Cuba, Rwanda, and Syria.[7] Other prohibitions are detailed in Exhibit 34.2.

For further reference, the reader is directed to the Federal Register and updates on the Federal Register, specifically Number 71, which provide more current and more detailed information.

(b) IMPORT DUTIES TO FOREIGN COUNTRIES. Duties at most other countries are higher than in the United States (average 13.8 percent of the value of the products), heightening the importance of awareness and compliance. Exhibit 34.3 lists duties or where to get information on them for the major economies of the world.

(c) EXPORT DOCUMENTS. The International Trade Administration (ITA) identifies a list of commonly required export documents that appear in Exhibit 34.4. The most common are the commercial invoice, the bill of lading, the insurance certificate, and the export packing list.

- *Denied Persons List:* A list of individuals and entities that have been denied export privileges. Any dealing with a party on this list that would violate the terms of its denial order is prohibited.
- *Unverified List:* A list of parties where BIS has been unable to verify the end use in prior transactions. The presence of a party on this list in a transaction is a red flag that should be resolved before proceeding with the transaction.
- *Entity List:* A list of parties whose presence in a transaction can trigger a license requirement under the Export Administration Regulations. The list specifies the license requirements that apply to each listed party. These license requirements are in addition to any license requirements imposed on the transaction by other provisions of the Export Administration Regulations.
- *Specially Designated Nationals List:* A list compiled by the Treasury Department, Office of Foreign Assets Control (OFAC). OFAC's regulations may prohibit a transaction if a party on this list is involved. In addition, the Export Administration Regulations require a license for exports or reexports to any party in any entry on this list that contains any of the suffixes ''SDGT,'' ''SDT,'' or ''FTO.''
- *Debarred List:* A list compiled by the State Department of parties who are barred by §127.7 of the International Traffic in Arms Regulations (ITAR) (22 CFR §127.7) from participating directly or indirectly in the export of defense articles, including technical data, or in the furnishing of defense services for which a license or approval is required by the ITAR.
- *Nonproliferation Sanctions:* Several lists compiled by the State Department of parties that have been sanctioned under various statutes. The Federal Register notice imposing sanctions on a party states the sanctions that apply to that party. Some of these sanctioned parties are subject to BIS's license application denial policy described in §744.19 of the EAR (15 CFR §744.19).
- *General Order 3 to Part 736 (page 9):* This general order imposes a license requirement for exports and reexports of all items subject to the EAR where the transaction involves Mayrow General Trading or entities related located in Dubai, United Arab Emirates.

Source: Department of Commerce, Bureau of Industry and Security.

EXHIBIT 34.2 LISTS OF PROHIBITIONS

Dual-use export licenses are required if the commodity falls into one of the following 10 types of dual-use materials:

1. Nuclear materials, facilities, and equipment
2. Materials, chemicals, microorganisms, and toxins
3. Materials processing
4. Electronics
5. Computers
6. Telecommunications and information security
7. Sensors and lasers
8. Navigation and avionics
9. Marine
10. Propulsion systems, space vehicles, and related equipment

Country	Tariff and/or Tariff Resource	Tax
Algeria	July 2003 Tariff Schedule from International Customs Tariffs Bureau	Value-added tax for some products is 7 percent. There is also a customs user fee of 4 percent.
Andean (Bolivia, Ecuador, Colombia, Peru, Venezuela)	September 2004 Tariff Schedule from International Customs Tariffs Bureau	
Angola	Online Tariff Schedule	There is a value-added tax of 2 to 30 percent depending on the good, applied on CIF + duty; additional fees include clearing costs (2% applied on CIF), revenue stamp (0.5% applied on FOB), port charges ($500/20-foot container or $850/40-foot container), and port storage fees (free for first 15 days but rarely do goods clear port within the grace period).
Argentina	Tariff info in Argentina changes daily. For most accurate info contact TIC at 1-800-USA-TRADE.	There is a 0.5 percent customs administration fee charged on CIF, and a 21 percent value-added tax applied on CIF + duty + customs fee. Some products may be subject to additional taxes; Specific duties are applied on many items.
Aruba	The basic customs duty in Aruba is 7.5 percent. In general, basic foodstuffs and raw materials for manufacturing are duty-free and luxury items are assessed at higher duties.	There is a 5 percent customs surchage and a 15 percent consumption tax applied on CIF + duty.
Australia	The duty is applied on the FOB value. APEC Tariff Database	There is a 10 percent goods and services tax applied on FOB + duty.
Austria	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 20 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 10 to 14 percent. The tax is applied on CIF + duty.
Bahamas	The basic ad valorem tariff rate is 35 percent tariff. Several products have separate rates. Duty is applied on CIF.	There is a 2 to 7 percent tax applied on CIF + duty.
Bahrain	Customs duties are imposed on the CIF value: 5 percent on foodstuffs and nonluxuries, 7 percent on consumer goods, 20 percent on cars and boats, 70 percent on tobacco products	Bahrain is essentially tax free, but a few products are subject to tax.
Bangladesh	Bangladesh Customs Schedule	15 percent value-added tax assessed on CIF + duty. Additional taxes are applied on luxury items.
Barbados	Duty rates range from 5 to 15 percent on all products except for primary agricultural products.	A 15 percent value-added tax is assessed on CIF + duty.
Belgium	April 2006 Tariff Schedule	There is a value-added tax of 21 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 1 to 12 percent. The tax is applied on CIF + duty.

EXHIBIT 34.3 DUTIES FOR MOST MAJOR ECONOMIES

Country	Tariff and/or Tariff Resource	Tax
Benin	August 2003 Tariff Schedule from International Customs Tariffs Bureau. The tariff rate is in the column marked CD.	There is a 15 to 20 percent value-added tax, a 1 percent statistical tax, and a 1 percent community solidarity levy. Agricultural, industrial, agro-industrial, livestock breeding, and fishing industry products may be subjected to additional taxes.
Bermuda	Bermuda Customs Tariff Schedule	No tax collected on products entering Bermuda.
Bolivia	April 2003 Tariff Schedule from Inter-American Development Bank	There is a 13 percent value-added tax. There is a 1.94 customs users fee.
Brazil	Tariff info in Brazil changes daily. For most accurate info, contact TIC at 1-800-USA-TRADE.	There is a Industrial Product Tax (IPI) (Federal sales tax) that ranges between 5 and 15 percent and a Merchandise Circulation Tax (ICMS) (state sales tax) that is generally around 18 percent. There is also a 1 percent miscellaneous tax. In addition, there is a Social Security tax that varies by product but is approximately 10 percent.
Brunei	ASEAN Tariff Database	No known taxes.
Burkina Faso	August 2003 Tariff Schedule from International Customs Tariffs Bureau. The tariff rate is in the column marked CD.	There is a 15 to 20 percent value-added tax, a 1 percent statistical tax, and a 1 percent community solidarity levy. Agricultural, industrial, agro-industrial, livestock breeding, and fishing industry products may be subjected to additional taxes.
Cambodia	ASEAN Tariff Database	There is a 10 percent value-added tax for most products.
Cameroon	There is a 5 percent duty on basic necessities, 10 percent on raw materials and capital goods, 20 percent on intermediate and miscellaneous goods, and 30 percent on consumer goods.	There is an 18.7 percent value-added tax on CIF + duty.
Canada	Tariff Resources: Canadian Customs Schedule	As of July 1, 2006, there is a 6 percent goods and services tax assessed on the duty-paid value (FOB + import duty). Commercial shipments to the provinces of New Brunswick, Newfoundland, and Nova Scotia are also subject to an additional 8 percent.
Central African Republic	There is a 5 percent duty on basic necessities, 10 percent on raw materials and capital goods, 20 percent on intermediate and miscellaneous goods, and 30 percent on consumer goods.	Tax information is not available.
Chad	There is a 5 percent duty on basic necessities, 10 percent on raw materials and capital goods, 20 percent on intermediate and miscellaneous goods, and 30 percent on consumer goods.	There is an 18.7 percent value-added tax on CIF + duty.

EXHIBIT 34.3 (*continued*) DUTIES FOR MOST MAJOR ECONOMIES

Country	Tariff and/or Tariff Resource	Tax
Chile	On January 1, 2004 the U.S.-Chile Free Trade Agreement went into effect. Items qualifying as U.S. originating would have a tariff between 0 and 6 percent. Almost all nonqualifying products have a 6 percent duty applied on CIF. Tariff Resource: January 2005 Tariff Schedule	There is a value-added tax of 19 percent applied on CIF + duty.
China	Market Access and Compliance Tariff Schedule	There is a value-added tax of 17 percent for most items, necessities such as agricultural products and utilities. Necessities, such as agricultural products and utilities, are taxed at 13%. Small businesses (annual production sales of less than RMB 1 million or annual wholesale or retail sales of less than RMB 1.8 million) are subject to VAT at the rate of 6 percent. Also, consumption tax (2 to 3 percent) provincial tax, applied on CIF; and excise taxes on alcoholic beverages, spirits, cigarettes, etc. range from 20 to 40 percent.
Colombia	May 2006 Tariff Schedule from International Customs Tariff Bureau	
Congo, Democratic Republic of	There is a 5 percent duty on basic necessities, 10 percent on raw materials and capital goods, 20 percent on intermediate and miscellaneous goods, and 30 percent on consumer goods. August 2004 Tariff Schedule from International Customs Tariff Bureau	There is an 18.7 percent value-added tax applied on CIF + duty.
Congo, Republic of	There is a 5 percent duty on basic necessities, 10 percent on raw materials and capital goods, 20 percent on intermediate and miscellaneous goods, and 30 percent on consumer goods.	There is an 18.7 percent value-added tax applied on CIF + duty.
Costa Rica	October 2003 Tariff Schedule from International Customs Tariff Bureau	Most products are subject to a 14 percent sales tax applied on CIF + duty.
Côte D'Ivore	August 2003 Tariff Schedule from International Customs Tariffs Bureau. The tariff rate is in the column marked CD.	There is a 15 to 20 percent value-added tax, a 1 percent statistical tax, and a 1 percent community solidarity levy. Agricultural, industrial, agro-industrial, livestock breeding, and fishing industry products may be subjected to additional taxes.
Cyprus	April 2006 Tariff Schedule from International Customs Tariff Bureau of European Union Customs web site	In most cases, value-added tax is 15 percent. There is a reduced rate of value-added tax of 5 percent that refers mainly to food and agricultural products. Value-added tax is charged on assets and services in Cyprus as well as on imports into Cyprus.
Czech Republic	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	The standard value-added tax rate is 19 percent and applies to most goods and services; a reduced rate of 5 percent applies to certain services and essential goods.

EXHIBIT 34.3 (*continued*) DUTIES FOR MOST MAJOR ECONOMIES

Country	Tariff and/or Tariff Resource	Tax
Denmark	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 25 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 0 percent. The tax is applied on CIF + duty.
Dominican Republic	April 2003 Tariff Schedule from Inter-American Development Bank	There is a value-added tax (ITBIS tax) of 16 percent applied on CIF + duty. There is also a 13 percent exchange commission applied on all imports (FOB value). There is an additional excise tax on alcohol, soft drinks, matches, cigarettes, cigars, perfumes, jewelry, and carpets, applied on CIF + duty.
Ecuador	Cotecna's Ecuador Tariff Book	Most products are subject to a 12 percent tax applied on CIF + duty.
EI Salvador	EI Salvador's Tariff Schedule. Type the first four or six digits of the HS Number in the box labeled ''codigo.'' The tariff rate is in the column labeled DAI.	There is a value-added tax of 13 percent applied on CIF + duty.
Equatorial Guinea	There is a 5 percent duty on basic necessities, 10 percent on raw materials and capital goods, 20 percent on intermediate and miscellaneous goods, and 30 percent on consumer goods.	Tax information is not available.
Estonia	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	The standard rate of value-added tax in Estonia is 18 percent. There are reduced rates of 0 percent and 5 percent.
Finland	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 22 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 8 to 17 percent. The tax is applied on CIF + duty.
France	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is value-added tax of 19.6 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 2.1 to 5.5 percent. The tax is applied on CIF + duty.
Germany	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is an Import Turnover Tax (in lieu of domestic value-added tax) of 17 percent for most products. Some products, such as basic necessities and agricultural foodstuffs, qualify for a reduced rate of 7 percent. The tax is applied on CIF + duty.
Ghana	Cotecna's Ghana Tariff Book	There is a 12.5 percent value-added tax on most products applied on CIF + duty. There are additional taxes on some products.
Greece	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 18 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 4 to 8 percent. The tax is applied on CIF + duty.
Guatemala	September 2003 Tariff Schedule from International Customs Tariffs Bureau. The tariff rate is in the column marked SAC.	There is a value-added tax of 12 percent applied on CIF + duty.

EXHIBIT 34.3 (*continued*) DUTIES FOR MOST MAJOR ECONOMIES

Country	Tariff and/or Tariff Resource	Tax
Guinea Bissau	August 2003 Tariff Schedule from International Customs Tariffs Bureau. The tariff rate is in the column marked CD.	There is a 15 to 20 percent value-added tax, a 1 percent statistical tax, and a 1 percent community solidarity levy. Agricultural, industrial, agro-industrial, livestock breeding, and fishing industry products may be subjected to additional taxes.
Honduras	April 2003 Tariff Schedule from Inter-American Development Bank	There is a value-added tax of 12 percent applied on CIF + duty. There is also a 0.5 percent service charge applied on all items except for raw material and some capital goods. There is also a 20 to 50 percent excise tax applied to alcohol and cigarettes.
Hong Kong	There is no duty for products shipped to Hong Kong.	Taxes are assessed only on automobiles, gasoline, tobacco, and alcohol.
Hungary	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	In most cases, value-added tax is payable at a rate of 25 percent. There is a reduced rate of 12 percent that relates mainly to some products and services.
Iceland	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 24.5 percent on most products applied on CIF + duty. There are additional taxes on some products.
India	2005 Tariff Schedule	There is a 1 percent landing charge applied on CIF, as well as taxes by the city, state, and central authorities respectively that total roughly 22 percent applied on CIF + duty + landing charge, but could be as much as 26 percent.
Indonesia	ASEAN Tariff Database	There is a value-added tax of 10 percent applied on CIF + duty. There is an additional sales tax on some luxury items.
Iraq	There is no tariff for products going to Iraq.	Effective March 1, 2004, a reconstruction levy of 5 percent of the total taxable customs value of all goods imported into Iraq from all countries will be applied. Exceptions are food, medicine, clothing, books, humanitarian goods; goods imported by the CPA, coalition forces, reconstruction contractors, NGOs, international organizations, diplomats, and coalition governments
Ireland	April 2006 Tariff Schedule from International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 21 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 4.2 to 12.5 percent. The tax is applied on CIF + duty.
Israel	Israel's Customs Tariff Schedule	There is a value-added tax of 18 percent applied on CIF + duty. Additional taxes may apply on some products.

EXHIBIT 34.3 (*continued*) DUTIES FOR MOST MAJOR ECONOMIES

Country	Tariff and/or Tariff Resource	Tax
Italy	April 2006 Tariff Schedule from the International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 20 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 4 to 10 percent. The tax is applied on CIF + duty.
Japan	APEC's Japan Tariff Schedule	There is a 5 percent consumption tax applied on CIF + duty.
Jordan	Jordan's Customs Tariff Table	There is a value-added tax of 13 percent applied on CIF + duty.
Kenya	Cotecna's Kenya Tariff Book	There is an 16 percent value-added tax applied on FOB + duty.
Kuwait	There is a 5 percent duty applied on most products. Cigarette and tobacco products have a 70 percent duty.	There are no taxes on products shipped to Kuwait.
Laos	ASEAN Tariff Database	There is a 10 percent tax applied on CIF + duty. Some products are subject to additional taxes.
Latvia	April 2006 Tariff Schedule from the International Customs Tariff Bureau or European Union Customs web site	The standard rate of value-added tax in Latvia is 18 percent. There are reduced rates of 0 percent to 9 percent.
Lebanon	January 2004 Tariff Schedule from the International Customs Tariffs Bureau or Government of Lebanon Customs Tariff	There is a 10 percent value-added tax on CIF + duty.
Lithuania	April 2006 Tariff Schedule from the International Customs Tariff Bureau or European Union Customs web site	In most cases, value-added tax in Lithuania is 18 percent; there is a reduced rate of 9 percent that applies to heating services. Value-added tax on transport services in Lithuania is 5 percent.
Luxembourg	April 2006 Tariff Schedule from the International Customs Tariff Bureau or European Union Customs web site	There is a value-added tax of 15 percent for most products. Some products, such as basic necessities and foodstuffs, qualify for a reduced rate of 3 to 12 percent. The tax is applied on CIF + duty.
Madagascar	October 2003 Tariff Schedule from the International Customs Tariffs Bureau	There is a value-added tax of 20 percent applied on CIF + duty. There may be additional import taxes applied as well.
Malaysia	ASEAN Tariff Database	Sales tax varies by product: 5, 10, or 15 percent with 10 percent being the most common. It is applied on CIF + duty.
Mali	August 2003 Tariff Schedule of the International Customs Tariffs Bureau. The tariff rate is in the column marked CD.	There is a 15 to 20 percent value-added tax, a 1 percent statistical tax, and a 1 percent community solidarity levy. Agricultural, industrial, agro-industrial, livestock breeding, and fishing industry products may be subjected to addtional taxes.
Malta	April 2006 Tariff Schedule from the International Customs Tariff Bureau or European Union Customs web site	18 percent value-added tax unless item is listed as exempt or at reduced rate: 5 percent value-added tax for confectionery and similar items; food and pharmaceutical products are exempt from import tax.
Mauritius	Mauritius integrated Customs Tariff Schedule	15 percent value-added tax assessed on most items with some exceptions; see schedule for value-added tax in addition to customs duty.

Source: U.S. Department of Commerce, Trade Information Center.

EXHIBIT 34.3 (*continued*) DUTIES FOR MOST MAJOR ECONOMIES

- *Shipper's Export Declaration (SED).* The SED is available through the Government Printing Office and a number of other commercial outlets. It can be electronically field using AESDirect.
- *Dual-use export controls and licenses.* Licensing is required for dual-use exports (commercial items that could have military applications) or exports to embargoed countries. In Europe, this is codified in EU Council Regulation 3381/94/EEC on the control of export of dual-use goods. Export control classification numbers (ECCNs) are used in many documents to determine whether an export license is needed.
- *Defense trade export controls and licenses.* In the case of defense export transactions (defense articles such as munitions), any person or company that intends to export such an article must first obtain approval from the U.S. Department of State Directorate of Defense Trade Controls (DDTC) prior to the export. The appropriate license form must be submitted to the DDTC for the purpose of seeking approval. In most cases, in order for a license to be considered, you first must be registered with the DDTC.
- *Commercial invoice.* This is a bill for the goods from the seller to the buyer. These invoices are often used by governments to determine the true value of goods when assessing customs duties. Governments that use the commercial invoice to control imports will often specify its form, content, number of copies, language to be used, and other characteristics.
- *Certificate of origin.* The certificate of origin is required by only some countries. In many cases, a statement of origin printed on company letterhead will suffice. Special certificates are needed for countries with which the United States has special trade agreements, such as Mexico, Canada, and Israel.
- *Bill of lading.* This is a contract between the owner of the goods and the carrier (as with domestic shipments). For vessels, there are two types: a straight bill of lading, which is nonnegotiable, and a negotiable or shipper's order bill of lading. The latter can be bought, sold, or traded while the goods are in transit. The customer usually needs an original as proof of ownership to take possession of the goods.
- *Insurance certificate.* Used to assure the consignee that insurance will cover the loss of or damage to the cargo during transit, an insurance certificate can be obtained from your freight forwarder.
- *Export packing list.* Considerably more detailed and informative than a standard domestic packing list, an export packing list itemizes the material in each individual package and indicates the type of package, such as a box, crate, drum, or carton. Both commercial stationers and freight forwarders carry packing list forms.
- *Import license.* Import licenses are the responsibility of the importer. Including a copy with the rest of your documentation, however, can sometimes help avoid problems with customs in the destination country.
- *Consular invoice.* Required in some countries, it describes the shipment of goods and shows information such as the consignor, consignee, and value of the shipment. If required, copies are available from the destination country's embassy or consulate in the United States.
- *Air waybills.* Air freight shipments are handled by air waybills, which can never be made in negotiable form.
- *Inspection certification.* Required by some purchasers and countries in order to attest to the specifications of the goods shipped, this is usually performed by a third party and often obtained from independent testing organizations.
- *Dock receipt and warehouse receipt.* These are used to transfer accountability when the export item is moved by the domestic carrier to the port of embarkation and left with the ship line for export.
- *Destination control statement.* This appears on the commercial invoice and the ocean or air waybill of lading to notify the carrier and all foreign parties that the item can be exported only to certain destinations.

Source: U.S. Department of Commerce, International Trade Administration.

EXHIBIT 34.4 COMMON EXPORT DOCUMENTS

34.5 HAZARDOUS MATERIALS

The shipment of hazardous and regulated goods across international borders is subject to regulation by international treaties. For transport of hazardous materials inside the United States, the Federal Hazardous Materials Law defines and classifies hazardous materials and articulates rules in these areas: hazard communication (Part 172, Subparts C–G); packaging requirements (Parts 173, 178, 179, and 180); operational rules (Parts 171, 173, 174, 175, 176, and 177); and training (Part 172, Subpart H). Also, Title 49 CFR Parts 100–185 address hazardous material classification, packaging, emergency response, and training.

Munitions are governed by the International Traffic in Arms Regulations (ITAR 120.3 and 120.4), which determine what articles are considered munitions.

Pharmaceuticals are subject to strict control internationally and in the United States. The U.S. Drug Pedigree Rule in the Prescription Drugs Marketing Act (PDMA), which takes effect in 2007, requires drugs to have a complete transfer and history record. There are also specific laws addressing guidelines for transporting anthrax and anthrax-contaminated objects and materials.[8]

Blood and biomedical products are restricted by the Biological and Toxin Weapons Convention of 1972, which instituted strict controls on biological agents so they could not be used to make weapons. The World Federation for Culture Collections Guidelines set conditions on shipments, including:

- Acceptance of written orders only.
- Notification to the Federation of shipments and purpose.
- Record keeping of mandated safety measures and compliance.
- Information to requestors of regulated organisms that they are prohibited from distributing materials to third parties.
- Refusal of delivery if the end-user certificate is incomplete.
- In all cases of doubt, the relevant national authority must be contacted.

Applicable U.S. regulations on the transport and trade of biohazards include the items that follow. Note that any observation that causes a shipper to question container integrity requires an incident report, DOT Form F 5800.1.

- CFR Title 33, Navigation and Navigable Waters, Parts 1–109
- CFR Title 46, Shipping, Parts 1–195
- CFR Title 49, Transportation, Parts 100–199 and 300–399
- International Civil Aviation Organization (ICAO) Technical Instructions for the Safe Transportation of Dangerous Goods by Air

34.6 OTHER GENERALLY ACCEPTED PROTOCOLS AND STANDARDS

The financial community has developed standards that codify and simplify transactions, particularly through incoterms and letters of credit. Incoterms are a uniform language classification system for international trade that codifies various combinations of buyer and seller responsibilities.

(a) INCOTERMS. Exhibit 34.5 classifies the various combinations of responsibilities codified in standard incoterms. In the simplest configuration, the buyer is responsible for all expenses under ex works (EXW) terms or the seller is responsible for all expenses under delivery duty paid (DDP) terms. Common terms are free on board (FOB), in which the seller pays up to the port of embarkation, and cost, insurance, and freight (CIF), in which the seller pays up to the port of debarkation. The title and risk pass from the seller to the buyer at different points for each incoterm. The International Chamber of Commerce in Paris periodically updates the incoterms to reflect the shifts of traffic across modes of transport, the influence of freight intermediaries and technology on standard terms, and similar factors.

(b) LETTERS OF CREDIT. Letters of credit essentially guarantee sellers that they will receive their money when the goods reach the buyer. And because the letter of credit is executed before shipment begins, the buyer is assured of receiving the product. The most common type of letter of credit is a commercial letter of credit, which is for a standard one-time payment. Commercial letters of credit are supported by shipping documents and bills of lading. Another type of letter of credit is a standby letter of credit, whereby the buyer deposits money and the seller withdraws money as the material or service is delivered.

34.7 THE INCREASING IMPORTANCE OF CONFORMANCE TO CUSTOMER STANDARDS

In addition to legal, structural, and procedural norms, shippers must often abide by customers' standards of compliance. In the retail trade, retailers write extensive documents outlining exactly what procedures suppliers should follow when shipping/routing deliveries to the companies. These routing guides stipulate detailed procedures for:

- Labeling (location and level of specificity)
- Specific carriers for different regions
- Paperwork specifications
- Delivery configuration (pallet specs, height, weight)
- Timeliness of deliveries
- Electronic Data Interchange (EDI) protocols
- Notification rules
- Invoicing
- Scheduling

Customer standards often come with penalties or deductions from invoiced amounts for noncompliance to any of the aforementioned logistical specifications. These can be small for minor incidents such as labeling errors, or large for other mistakes such as incorrect items or missed delivery time windows.

Acronym	EXW	FCA	FAS	FOB	CFR	CIF	CPT	CIP	DAF	DES	DEQ	DDU	DDP
Prefix	Ex Works	Free Carrier	Free Alongside Ship	Free Onboard Vessel	Cost and Freight	Cost, Insurance, and Freight	Carriage Paid To	Carriage Insurance Paid To	Delivered at Frontier	Delivered	Delivered Ex Quay Duty Unpaid	Delivered Duty Unpaid	Delivered Duty Paid
Suffix	Named place	Named place	Port of destination	Port of destination	Place of destination	Place of destination	Place of destination	Port of destination	Named place	Port of destination	Port of destination	Place of destination	Port of destination
Warehouse Storage	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Warehouse Labor	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Export Packing	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Loading Charges	Buyer	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Inland Freight	Buyer	Buyer	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Terminal and Port Receiving Charges	Buyer	Buyer	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Forwarder's Fees	Buyer	Buyer	Buyer	Buyer	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Loading on Vessel	Buyer	Buyer	Buyer	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Ocean/Air Freight	Buyer	Buyer	Buyer	Buyer	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller	Seller
Charges on Arrival at Destination	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Seller	Seller	Buyer	Buyer	Seller	Seller	Seller
Duty, Taxes, and Customs Clearance	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Seller
Delivery to Destination	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Buyer	Seller	Seller

EXHIBIT 34.5 BUYER AND SELLER RESPONSIBILITIES UNDER INCOTERMS

34.8 CONCLUSION

Increasing security regulation has defined the environment for shipper compliance since 9/11/2001. Today, shippers must respect the impact that new trade rules, documentation requirements, and inspection authorities may have on the speediness and administrative burden of shipping products, especially internationally. In the future, however, these factors are likely to fade into standard operating procedure, and other issues will supersede them, such as the standardization of information and financial transmission protocols and more stringent customer delivery requirements that facilitate on-demand global logistical flows.

Notes

1. Three other government agencies indirectly affect shipper compliance. The Department of Commerce—International Trade Administration (ITA) investigates unfair trade and dumping. The International Trade Commission, an independent federal agency, publishes the Harmonized Tariff Schedule and provides trade policy analysis. And the Patent and Trademark Office (PTO) investigates disputes involving the illegal import or export of intellectual property.
2. Based on an analysis of the latest available U.S. Census data regarding imports (1993).
3. Based on an analysis of the U.S. International Trade Commission tariff report (2006).
4. These are adapted from lists made available by the U.S. Customs and Border Protection.
5. 19 U.S.C. 1431(c)(1) states that each importer or consignee's name and address must be made available for public disclosure except with express authorization of the CBP. Carriers and non-vessel operating common carriers (NVOCCs) cannot list their own names in lieu of the name of the consignee in order to conceal the identity of their customer.
6. The Final Rule was issued on April 22, 2005.
7. Export Administration Regulations Part 746, August 31, 2006.
8. Pipeline and Hazardous Materials Safety Administration (PHMSA) Guidelines for Transporting Anthrax and Anthrax-Contaminated Objects and Materials.

CHAPTER 35

PHARMACEUTICAL

James G. Robertson

Manufacturing, research, design, development, marketing, and many operations in the pharmaceutical industry have been regulated in the United States since 1906 when the U.S. Food and Drug Administration (FDA) was created by passage of the Food and Drugs Act. This act has been amended significantly 19 times, is supplemented by 23 other acts, and is now known as the Federal Food, Drug, and Cosmetic Act. Under the authority created by these acts, the FDA has made over 1,000 rules in Title 21 of the Code of Federal Regulations (CFR). The FDA mission statement asserts that the FDA "is responsible for protecting the public health by assuring the safety, efficacy, and security of human and veterinary drugs, biological products, medical devices, our nation's food supply, cosmetics, and products that emit radiation." This scope of regulation is very broad, and together it encompasses around a quarter of the U.S. economy.

Similar regulations are in place in other developed countries and regions, including Canada, Europe, Australia, and Japan. Emerging economies typically rely on regulations from the World Heath Organization (WHO).[1] These align reasonably well with those from the United States and other developed countries. Europe and some other countries also require registration of manufacturers for compliance with certain ISO standards. The international regulators are outlined later in this chapter after first explaining the approach in the United States.

The pharmaceutical sector includes the drug, biological, and device (implantable, therapeutic, and diagnostic) product categories. Some regulations are specific to each of these categories, but many, including those over information

security, apply universally to the whole industry. The FDA organization includes four centers that are concerned with pharmaceutical products:

1. Center for Biologics Evaluation and Research (CBER)
2. Center for Devices and Radiological Health (CDRH)
3. Center for Drug Evaluation and Research (CDER)
4. Office of Regulatory Affairs (ORA)

The product development and FDA approval processes are different in each center, but the manufacturing operations for all are covered by specific good manufacturing practice (GMP) regulations in 21 CFR Part 211. Devices are also covered by a quality system regulation, 21 CFR Part 820, that aligns with ISO 9000.[2] Most U.S. device companies also meet ISO 13485[3] for the European market. The FDA has issued guidance recommending similar quality system concepts for drugs and biologics in addition to the other rules that already apply there. The entire spectrum of a pharmaceutical product's life cycle is regulated, from the acquisition of raw materials through use to the disposition of unused or outdated product.

Information technology (IT) is essential to the entire pharmaceutical sector for manufacturing automation, laboratory operations, regulatory processes, and quality system administration as well as the more typical business applications, including manufacturing execution systems (MES) and enterprise resource planning (ERP) systems. Along with the use of IT comes a risk that information will be compromised or not available when needed. This can result from failures, mistakes, malware (software designed to destroy, aggravate, wreak havoc, hide potentially incriminating information, and/or disrupt and damage computer systems), crimeware (class of computer program designed specifically to automate financial crime), maintenance, or intrusions. Such compromises to information have the potential to lead to harm to the public. In 1983, in response to the increasing use of PCs in pharmaceutical manufacturing, the FDA published a guidance document on the use of computerized systems. In 1997, it followed that with a rule, 21 CFR Part 11, which establishes a system of controls over IT, software, and computerized systems to mitigate the risks to information security. Security of information here is used in accordance with the meaning given in the ISO 17799 standard as integrity, confidentiality, and availability. The controls introduced by Part 11 were interpreted and focused by numerous guidance documents published by the FDA. Most notable of these is the August 2003 "Guidance of Industry Part 11, Electronic Records: Electronic Signatures—Scope and Application," which narrows the scope to only those records that are required by other FDA regulations, called the predicate rules. Such records are often referred to as Part 11 records. Typical applications that process Part 11 records in pharmaceutical operations include:

- Document management
- Maintenance and preventive maintenance management
- ERP systems

- Quality system execution
- Clinical trial activities and records[4]
- Laboratory operations and records
- Shipping and receiving
- Inventory management
- Computerized manufacturing equipment

In addition to the Part 11 rule, the FDA requires that software, computers, and the equipment used in manufacturing or in the quality system be validated. The validation is to verify that the equipment, software, and systems operate as intended and that the necessary processes are in place to maintain their operational status. These processes include policies, procedures, training programs, auditing, reporting, change management, access controls, and preventive maintenance. Validation as practiced in the pharmaceutical industry is roughly equivalent to a combination of accreditation and testing as prescribed by the IT controls in the CobiT[5] framework from the Information Technology Governance Institute (ITGI).

Equipment that delivers medication such as infusion pumps, performs diagnostic functions such as with X-ray or MRI scanners, monitors patients, or is implanted in the body is a device in the meaning of 21 CFR Part 820. Custom software that is used to process Part 11 records is considered a device by the FDA for regulatory purposes, and the software development life cycle (SDLC) of Part 820 applies. Safety of devices is a major concern of regulators. Hazards can be presented from electrical, mechanical, material, software, and functional sources. The International Electrotechnical Commission (IEC)[6] rule 60601-1 addresses methods to mitigate many of these safety risks and is the standard used by the major countries. Exhibit 35.1 shows the countries that have adopted this IEC 60601-1 rule and under what names. More on this subject can be found in "A Primer for IEC 60601-1."[7]

The Global Harmonization Task Force (GHTF),[8] established by the United States, Canada, Australia, Japan, and the European Union, lends credence to using the IEC 60601-1 standard as the model for compliance of electrical medical devices. In the United States, the FDA recognizes IEC 60601-1 as a consensus

Country	IEC 60601-1 adopted as
United States	ANSI/UL 2601-1 (U.S. national deviations)
Canada	CAN/CSA C22.2 No. 601.1 (Canadian national deviations)
European Union	EN 60601-1 (identical to IEC 60601-1); in United Kingdom, BS EN 60601-1
Japan	JIS T0601-1 (Japanese national deviations)
Australia/New Zealand	AS/NZ 3200.1 (Australian and New Zealand national deviations)

Exhibit 35.1 Countries That Have Adopted IEC 60601-1

standard with any amendments, and with specific national alterations, such as ANSI/UL 2601-1. More information regarding the CDRH's consensus standards can be found on the FDA web site.[9] The embedded software, and/or firmware, in devices is similar to custom software and should be developed following an SDLC method in line with the FDA guidance on software validation.[10] This SDLC process draws on standards from the Institute of Electrical and Electronic Engineers (IEEE)[11] and standards from other organizations such as the National Institute of Standards and Technology (NIST).

Devices in a hospital or doctor's office that are on a network, such as imaging or diagnostic equipment, also pose risks to information security. To address some of these, the FDA has issued special guidance[12] for cybersecurity. Devices that include software as embedded components also come under tight scrutiny, as failures in some of these have the potential of causing death. The FDA looks to its own guidance documents as well as to the IEC for practices that companies should follow in developing such software. Such controls must be demonstrated as part of the application to the FDA for approval of devices with embedded software.

As of this writing, the FDA is preparing an updated version of the Part 11 rule, which is expected to be in line with the recent guidance it has published and to incorporate some aspects of the U.S. Federal Information Security Management Act of 2002 (FISMA). The FISMA rule applies to U.S. government agencies and those companies that do business with them. FISMA required NIST to develop a set of IT controls, which are now published as SP800-53.

Janet Woodcock, deputy commissioner of the FDA,[13] reported that the incidents of patient harm are far greater in the health care delivery system than those from product defects. The harm comes from a combination of factors, including use error, medication error, and medication interactions. A broader use of information systems in the health care delivery system should help reduce these errors. Ultimately a nationwide or broader database of patient records will likely be operating to provide instant access to a patient's complete history, X-ray images, scans, medications, conditions, and so on. It is estimated that greater use of IT in the delivery of health care would bring a 30 percent reduction in the cost of health care in the United States. Before such information technology can be implemented and accepted by the public, it must achieve a very high level of security so that the patient records are accurate, confidential, and available where and when needed. Such systems will demand very secure and controlled access to avoid abuse and ensure privacy, as addressed by the HIPAA security rule.[14]

Good automated manufacturing practices (GAMP) is a method of validating computerized systems and IT infrastructures that was developed in England and published in the United States by the Institute of Pharmaceutical Engineers (ISPE). This GAMP method is widely used in the United States and in Europe for validating the pharmaceutical manufacturing systems. It employs a

life cycle process similar to that required for device software development that includes documented requirements, design specifications, risk assessment, change management, and continuity processes such as backups. The life cycle process leads to a comprehensive testing regime, followed by an operations phase where validated status is maintained by managing and documenting change. Testing is done to show that the systems perform their intended functions and also show that the operating personnel can operate the systems correctly according to the written procedures. This GAMP method is primarily focused on equipment but has been extended to cover the validation of IT infrastructure and IT applications. The IT control frameworks such as CobiT, Information Technology Infrastructure Library (ITIL),[15] or the NIST SP800-53 provide a more robust model with more focus on governance than does GAMP.

The measures taken by the FDA to mitigate the risks to public health from information technology have a lot in common with the IT frameworks used to meet requirements of the Sarbanes-Oxley Act (SOX) and the requirements of the Public Company Accounting Oversight Board (PCAOB). The IT controls applied for SOX can be tailored to also satisfy some of the FDA requirements where there are overlaps of system functions such as can be found with ERP systems. Some companies have successfully mapped controls from CobiT[16] for SOX to the controls required by Part 11. Similarly, since the controls of ITIL and other frameworks can be mapped to CobiT, a lot of commonality can be found between the FDA Part 11 rule and other recognized IT control frameworks.

The terms *IT governance*[17] and *IT control,* while common in the business and accounting communities, are not necessarily common in pharmaceutical operations. These are roughly equivalent to the FDA "Quality System Regulation"[18] when implemented according to the quality system guidance.[19] Governance roughly equates to the FDA expectation of validation combined with an internal auditing process and periodic inspections by the FDA. CobiT states, "The IT Governance process includes the information systems strategic plan, the IT risk management process, compliance and regulatory management, and IT policies, procedures, and standards." CobiT for SOX wraps this with monitoring and reporting into the overall IT control environment.

Many countries require that any pharmaceuticals provided to citizens comply with internal regulations and be approved by the country's internal pharmaceutical regulatory body. In order to market any pharmaceutical in the United States, the facility producing it must meet the FDA requirements and be approved by the FDA. Similarly, the pharmaceutical product itself must also be approved by the FDA for sale and use in the United States. This is true regardless of the country where the facility is located or the corporate ownership. Conversely, for a U.S.-owned firm to market a drug in any other country, that drug must be approved for sale there and the facility producing it must meet that country's regulations.

Those pharmaceutical companies that want to market products into multiple countries invariably are required to obtain approvals for the drug itself in each country and then meet the good manufacturing practice (GMP) and other regulatory requirements in the country where the manufacturing is performed. The costs of meeting multiple regulatory requirements and obtaining multiple approvals can multiply and ultimately become a critical factor in business decisions about which markets to serve. This cost of multiple regulatory environments leads to considerable interest on the part of manufacturers to achieve comity or a level of mutual recognition between the regulatory requirements and processes in various countries. To this end, the International Congress on Harmonization (ICH),[20] which is composed of both industry and country regulatory body members from the United States, Europe, and Japan, is working to establish common guidance. Some recent activities in that area include:

- "ICH Q27A Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients." This has been adopted by the FDA for GMP guidance in the handling of active pharmaceutical ingredients (APIs).
- "ICH Q8 Pharmaceutical Development." This guideline describes the suggested contents for the pharmaceutical development section of a submission in the ICH M4 Common Technical Document (CTD) format.
- "ICH Q9 Quality Risk Management." This is in the process of being adopted into the European regulatory system and is being referenced by the FDA. The application of quality risk management is optional, but hopes are that, if used correctly, significant benefits will result.

Internationally, the regulations governing pharmaceutical industries have evolved in parallel with those of the United States. The regulation programs in Europe, Japan, Australia, and Canada are among the most mature and in many ways have similar requirements as those of the United States although there are differences in details, inspections, and enforcement. The developing economies largely depend on WHO, which has established a set of GMP recommendations and related training programs for member states. Any country that complies with the regulations from Australia, Japan, Europe, or the United States will likely also meet many of the requirements of WHO.

While the United States leads in recognition of the need for information security and validation of computer systems, the other countries are increasingly adopting measures to address the need, particularly in Europe and the other more developed countries. Validation of computing systems is common in Europe, where Annex 11 of "The Rules Governing Medicinal Products"[21] sets down some general requirements for information security and addresses some of similar issues as 21 CFR Part 11 in the United States. The overall issue of information security does not appear to be as tightly bound to the pharmaceutical industry outside the United States as it is inside, but instead it is part of a more global recognition of the risks to information integrity.

Australia	Therapeutic Good Administration (TGA)
Canada	Health Products and Food Branch (HPFB)
	Canadian Medical Devices Conformity Assessment System (CMDCAS)
China	State Food and Drug Administration (SFDA)
Europe	European Medicines Agency (EMEA)
India	Central Drugs Standard Control Organization (CDSCO)
Japan	Ministry of Health, Labor, and Welfare (MHLW)

EXHIBIT 35.2 REGULATORY BODIES

35.1 INTERNATIONAL

The FDA web site lists over 200 international regulatory bodies[22] that hold some sway over the pharmaceutical and food regulations worldwide. The FDA's International Activities Coordinating Committee (IACC) serves to coordinate with international regulations. Australia, Canada, and the United States have cooperative agreements for GMP inspections. Exhibit 35.2 shows the regulatory bodies in some of the larger economies.

35.2 CANADA

Canada has 16 directorates under its Health Products and Food Branch (HPFB) that cover categories including drugs and biologics. Canada requires that certain medical devices be designed and manufactured under a registered quality management system (QMS) that meets the criteria of the international standards: ISO 13485-98 and ISO 13488-98. To implement these regulations, which came into force on January 1, 2003, the Canadian Medical Devices Conformity Assessment System (CMDCAS) was developed by Health Canada's Therapeutic Products Directorate (TPD), in collaboration with the Standards Council of Canada (SCC).

Canada and Australia have entered into a mutual recognition agreement whereby each country accepts the inspections done by the other.

35.3 EUROPE

The member states of the European Union (EU) each have their own national component authority under the umbrella of the European Agency for the Evaluation of Medicinal Product (EMEA).[23] The EMEA collects the inspection information but it does not do the actual inspections, instead relying for that on the national component authorities of the member states. Some limited mutual recognition agreements (MRAs) exist between the EU and New Zealand, Australia, Switzerland, Japan, and Canada; none exists with the United States. However, discussions are ongoing between the EU and the United States about achieving some mutual recognition.[24] The main responsibility of EMEA is the protection and promotion of public and animal health, through the evaluation and supervision of medicines for human and veterinary use. The EMEA coordinates the evaluation and supervision of medicinal products throughout the European Union. It brings together the

scientific resources of the 25 EU member states in a network of 42 national competent authorities. It cooperates closely with international partners, reinforcing the EU contribution to global harmonization.

The EMEA's Inspections Sector deals with a number of tasks laid down in Regulation (EC) 726/2004, specifically those concerned with the coordination of the verification of compliance with the principles of good manufacturing practice, good clinical practice (GCP), and good laboratory practice (GLP) and with certain other aspects of the supervision of authorized medicinal products in use in the European Community. EU-GMP principles and guidelines are laid down in Directive 2003/94/EC (human products) and 91/412/EEC (veterinary products). These principles and guidelines are subject to further detailed guidance in the form of the EU-GMP guide, with its annexes.

The European Conformity (CE) mark must be on any device place on the market in EU countries and for free movement within the European Free Trade Association (EFTA) and European Union. For device manufacturers, conformity includes registration under ISO 13485 or 13488.

35.4 ASIA

The growth that is occurring in Asia has increased the demand for pharmaceutical manufacturing both for domestic markets and for export. To meet these needs, new or improved regulations are being adopted throughout with the more stringent focus paid by those countries that want to export, particularly devices, to United States, EU, and other countries with strict controls. The Pacific Bridge Medical[25] association in Bethesda, Maryland, works with the Asian countries to help them ramp up their regulatory processes, including the adoption of rules and enhanced inspection. Some Asian countries that are improving their regulatory environments are China, Japan, Hong Kong, India, Taiwan, Vietnam, Philippines, and Malaysia.

(a) CHINA. China's State Food and Drug Administration (SFDA) is working to improve its regulatory environment and now requires all manufacturers to be GMP certified. The pharmaceutical and device industries in China are growing at about 10 percent annually and together are now valued at about $25 billion. In 2004 China implemented a program for Drug Safety Credit Classification, which rates domestic manufacturers based on their degree of compliance learned through inspections. Currently, the SFDA is implementing "General Rules on Good Manufacturing Practice (GMP) for Medical Devices" and "Implementation Guidelines for Disposable Sterile Medical Devices and Implanted Medical Devices." Currently there are about 10,000 small device-manufacturing companies in China and to export their products to developed countries they will need to implement quality systems that conform with the requirements of the target countries.

(b) JAPAN. Japan has recently implemented a new revision to its Pharmaceutical Affairs Law (PAL) and made changes to their Ministry of Health, Labor, and

Welfare (MHLW) to create a more efficient and transparent review process to bring safer and more reliable medical products to the market. These changes include risk-based classification, standard process for new drug applications, and ISO compliance. All companies selling products in Japan are required to be a market authorization holder (MAH). The MHLW has published a draft regulation on the requirements for in vitro diagnostic (IVD) devices.

(c) HONG KONG. Hong Kong has a voluntary risk-based regulatory process based on GHTF recommendations called the Medical Device Administrative Control System (MDACS). The MDACS is being implemented in phases as managed by the Medical Device Control Office (MDCO).

35.5 SUMMARY

The pharmaceutical industry is highly regulated and the cost of compliance is significant. In the United States the cost of operating the pharmaceutical device company quality organization averages around 7 percent to 9 percent of the cost of operations with outliers as low as 4 percent and as high as 14 percent. The average number is higher for drug and biotech companies. Skimping on quality substantially increases the risk of action by the FDA. These actions can include large fines (as high as $500 million so far) with third-party oversight while operating under consent decree. Sometimes companies choose to exit the market or abandon a product line as a consequence of FDA actions. Some companies with a history of recurring noncompliance can be shut down by the FDA.

In all of the larger economies there is an increasing shift toward commonality and mutual recognition, but at this time most countries still have their own regulations. The difference in the regulatory climate between developed and developing countries is large but closing. Concern about the security of information and integrity of software used in pharmaceutical operations is highest in the United States and Europe and increasing in other countries.

To help their local companies surmount the regulation hurdles, many developing countries are rapidly establishing regulations along with enforcement and inspection programs. The implementation of regulations alone does not immediately change the quality and reliability of products, though, as such changes require behavior adjustment and often capital expenditures that can take time to achieve.

Notes

1. World Health Organization, www.who.int/en/.
2. ANSI/ISO/ASQ Q9000-3-1997, "Quality Management and Quality Assurance Standards—Part 3: Guidelines for the Application of ANSI/ISO/ASQC Q9001-1994 to the Development, Supply, Installation, and Maintenance of Computer Software."
3. ANSI/AAMI/ISO 13485:2003, "Medical Devices—Quality Management Systems—Requirements for Regulatory Purposes."

4. FDA, "Guidance for Industry Computerized Systems Used in Clinical Trials," Draft Guidance, September 2004, Compliance Revision 1.
5. IT Governance Institute (ITGI), Information Technology Control Objectives (CobiT).
6. International Electrotechnical Commission, www.iec.ch.
7. Leonard Eisner, Robert M. Brown, and Dan Modi, "A Primer for IEC 60601-1," Eisner Safety Consultants, QuadTech Inc., and Alcon Research Inc.
8. Global Harmonization Task Force (GHTF; www.ghtf.org).
9. FDA CDRH Consensus standards: www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.
10. FDA, "General Principles of Software Validation; Final Guidance for Industry and FDA Staff," January 11, 2002.
11. IEEE Std 1074-1997, "IEEE Standard for Developing Software Life Cycle Processes."
12. FDA, "Guidance for Industry, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," January 2004.
13. Janet Woodcock, Deputy Commissioner for Operations, FDA, Presentation at AdvaMed Congress on Global Approaches to Risk Management, May 19, 2006.
14. "Health Insurance Reform: Security Standards," Department of Health and Human Services, Title 45 of the Code of Federal Regulations Parts 160, 162, and 164, Federal Register 68, no. 34, Thursday, February 20, 2003.
15. Information Technology Infrastructure Library (ITIL) from the British Office of Government Commerce (OGC).
16. IT Control Objectives for Sarbanes-Oxley.
17. The term *governance* carries varying meanings depending on context. The ITGI defines it as: "The leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives." Further, ITGI states: "IT governance is the responsibility of the board of directors and executive management."
18. FDA, "Quality System Regulation," for devices, 21 CFR 820; FDA, "Guidance for Industry Quality System Approach to Pharmaceutical Current Good Manufacturing Practice Regulations," Draft, September 2004.
19. FDA, "Guidance for Industry Quality System Approach to Pharmaceutical Current Good Manufacturing Practice Regulations," Draft, September 2004.
20. "The International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use," www.ich.org/cache/compo/276-254-1.html.
21. EU, European Commission, Directorate General III—Industry Pharmaceuticals and Cosmetics, "The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practices, Medicinal Products for Human and Veterinary Use, Annex 11, Computerized Systems." http//pharmacos.eudra.org/
22. FDA list of international regulatory bodies: www.fda.gov/oia/agencies.htm.
23. The European Medicines Agency is based in London. http://emea.europa.eu/I.
24. FDA Office of International Programs: www.fda.gov/oia/homepage.htm.
25. Pacific Bridge Medical, 7315 Wisconsin Ave., Suite 609E, Bethesda, MD 20814, Phone 301-469-3400, info@pacificbridgemedical.com.

CHAPTER 36

PUBLIC SECTOR TRANSPARENCY—HOW IS IT REGULATED IN EUROPE?

Massimiliano Claps

36.1 INTRODUCTION: THE ROLE OF TRANSPARENCY FOR GOOD GOVERNANCE

International institutions and policy science scholars have widely thought about what good governance means. For instance, in 2004, the Independent Commission on Good Governance in Public Services established by the UK Office for Public Management (OPM) and the Chartered Institute of Public Finance and Accountancy (CIPFA), identified a set of good governance standards for public services:

- Good governance means focusing on the organization's purpose and on outcomes for citizens and service users.
- Good governance means performing effectively in clearly defined functions and roles.
- Good governance means promoting values for the whole organization and demonstrating the values of good governance through behavior.
- Good governance means taking informed, transparent decisions and managing risk.
- Good governance means developing the capacity and capability of the governing body to be effective.
- Good governance means engaging stakeholders and making accountability real.

Among those principles, transparency of information occupies a primary role. As Thomas Jefferson said: "Information is the currency of democracy."

Transparency refers to the availability of information to the general public and clarity about government rules, regulations, and decisions. The difficulty with ensuring transparency is that only the generator of information may know about it, and may limit access to it. Hence, it may be useful to strengthen the citizens' right to information with a degree of legal enforceability. For similar reasons, broadly restrictive laws that permit public officials to deny information to citizens need to provide for independent review of claims that such denial is justified in the greater public interest. Greater transparency makes it difficult for government officials and politicians to ignore the interests of the general public when undertaking their duties, while at the same time enhancing citizen participation in politics and increasing competition among political parties. In practice, though, it may sometimes be necessary to place limits on the principle of transparency. In doing so, it may be helpful to distinguish information as a commodity from information as a process. For example, intellectual property rights may need to be protected in order to encourage innovation and invention; but decision making on the establishment of intellectual property and rights thereto (i.e., to whom they are granted and why) should be transparent.

36.2 RIGHT OF ACCESS TO PUBLIC SECTOR INFORMATION IN EUROPE

Western European governments have legislations that not only regulate the mechanisms of internal auditing, but also ensure all constituents have the right of access to administrative acts held by public authorities, to enforce the greatest possible transparency of their decision-making processes.

The European Union itself pushed forward the transparency agenda, by regulating the right of access to information on environmental matters. Council Directive 90/313/EEC of June 7, 1990, on the freedom of access to information on the environment initiated a process of change in the manner in which public authorities approach the issue of openness and transparency, establishing measures for the exercise of the right of public access to environmental information, which should be developed and continued. Directive 2003/4/EC of the European Parliament and of the Council of January 28, 2003, on public access to environmental information repealed Directive 90/313/EEC and expanded the right of access existing under the previous regulation.

(a) FRANCE. France was an early adopter of a freedom of information legislation in 1978 (Loi 78-753 du 17 Juillet 1978, Titre Ier: De la liberté d'accès aux documents administratifs). Article 1 states:

> The right of constituents to information is specified and guaranteed by this title with regard to freedom of access to the administrative documents of nonindividual nature. . . . Regarded as administrative documents within the meaning of the present title [are] all files, reports/ratios, studies, reports, official reports,

> statistics, directives, instructions, circulars, notes and ministerial answers, which comprise an interpretation of the substantive law or a description of the administrative procedures, opinion, except for the opinion of the Council of State and the administrative courts, forecasts and decisions, taking the form of writings, of sound or visual recordings, of digital proceedings of nonindividual information.

Article 2 indicates that all public authorities are subject to the regulation: administrations of the state, the local authorities, the publicly owned establishment and enterprises or the organizations, even if private, that are in charge of managing public services. Exceptions to the right of access include:

- The secrecy of the deliberations of the government and responsible authorities concerned with the executive power
- The secrecy of national defense and foreign policy
- Monetary and currency policy acts
- The safety of the state and public security
- The course of the procedures initiated in front of judicial authorities, or preliminary operations to such procedures, except authorization given by the proper authority
- The secrecy of the private life, as well as personal and medical files
- Commercial and industrial secrecy
- Tax and custom fraud control activities
- Other secrecy specifically protected by the law

(b) GERMANY. First approved by the Bundestag in early June, Germany's Freedom of Information (FOI) law was voted on July 8, 2005, by the Bundesrat. The new FOI regime entered into force in January 2006.

The new law provides the public with a general right to access federal government information. However, this general right is limited by a number of broadly defined exemptions, covering for instance security-sensitive issues, potential threats to public safety, and even the "fiscal interests of the Federal Government." In order to protect industrial secrets and intellectual property, documents containing information on a private company can be disclosed only with the consent of that company.

(c) ITALY. In 1990 the Italian parliament defined the rules guiding the modernization of the public administration (Legge 241/90 Norme in Materia di Procedimento Amministrativo e di Diritto di Accesso ai Documenti Amministrativi). Article 22 of the law states: "To ensure transparency and favor fair management of administrative processes, the right of access to administrative documents is guaranteed to anyone interested." The article also indicates that administrative document is any act deriving from the execution of administrative tasks, whatever is the format, graphic, photographic, or digital.

Article 23 indicates that central government departments, local authorities, other public institutions, and private companies in charge of providing public services are subject to the legislations. Exceptions to the application of article 22 include acts concerning:

- National security and defense and foreign policy
- Monetary and currency policy
- Public order and security
- The confidentiality of third parties, persons, groups, and enterprises

The law on the administrative transparency (Law 241/90) along with the legal validity of the electronic document, which was sanctioned by Law 59/1997, gave the push to the digital transformation of the Italian public administration. This culminated into issuing regulations on "Digital Signature" (DPR 513/97) and "Digital Protocol" (DPR 428/98). Such norms have been subsequently inserted in the Unified Body of Laws on administrative documentation (DPR 445/2000). The consequent development of digital signature and digital protocol tools, joined with the expansion of the use of e-mail, is rendering realization of a completely automated management of the flows of documents in the administrations. The Digital Protocol is the critical piece in terms of a push toward digitization of document and record management. The initiative follows the guidelines set by the Ministry for Innovation and Technologies in October 2003 (Decreto 14/10/2003) and has compelled all public administrations—public primary, secondary, and tertiary education institutions; central government organizations; regions, provinces, municipalities, and syndicates of local authorities; chambers of commerce; national health-care service agencies; and public corporations—to start to deploy document and record management and work flow systems since the beginning of 2004. The objectives are to:

- Automate registration of all documents
- Automate administrative work flow
- Digitize and archive all administrative documents
- Sign electronically administrative documents
- Grant transparent access to digitally archived documents and data
- Grant maximum security of handling and access to documents and data

Other regulations were issued (DPCM 31/10/2000 and 7 issued by AIPA/CR/28 May 2001) to set the technical rules to ensure interoperability between independent systems of protocol and between the protocol and digital signature and e-mail. Such rules, in particular, identify XML as the data format to codify the exchanged information, SMTP as the e-mail standard, and MIME as the form for transport of documents. Furthermore, deliberations n.42/2001 and n.11/2004 issued by AIPA (now CNIPA, the Italian center for IT in the public administration), set the technical indications for archiving and conservation of documents in digital format. These technical rules state, for instance, that: (1) Optical devices must be used—that is, devices written and read through laser technology (art. 1). Art. 8

indicates, however, that nonoptical technologies can be used, where they ensure the content cannot be changed relative to the original document. (2) Archiving must be coupled with a registry containing date and digital signature of the administrator for every file. (3) Copies must be maintained. (4) Any document can be archived digitally regardless of the format of the original data (paper, film, etc.). The sum of all those regulatory interventions creates a legislative framework that not only asks for transparency and right of access to information, but also dictates the rules for e-enabled administration.

(d) SPAIN. Law 30/1992 (Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común) dictates the principles that regulate administrative proceedings. Article 37 of the law states: "The citizens have the right to accede to the registries and the documents that are part of acts stored in public archives, whatever ... the form of expression, graphic, audio, or video, or the type of material support in which they appear, whenever such files correspond to procedures finished [by] the date of the request." The right of access does not cover information about individuals, which is instead regulated by privacy laws. Other exceptions to the right of access are:

- Acts that contain information on the performances of the government of the state or the autonomous communities, in the exercise of its constitutional competencies not subject to administrative right
- Acts that contain information on the national defense or the security of the state
- Acts relative to the investigation of crimes when this could put in danger the protection of the rights and liberties of third parties or the necessities of the investigations
- Matters protected by commercial or industrial secret
- Acts derived from the implementation of monetary policy

(e) UNITED KINGDOM. The Freedom of Information Act (FOI) enables people to gain access to information held by public authorities in two ways:

1. From January 1, 2005, people will have the right to make a request for any information held by a public authority and the authority will have to comply with the Freedom of Information Act in responding. Article 1 of the Act states: "Any person making a request for information to a public authority is entitled—
   - to be informed in writing by the public authority whether it holds information of the description specified in the request, and
   - if that is the case, to have that information communicated to him."
2. Prior to that, in the run-up to January 2005, every public authority had to make some information available as a matter of course through a

publication scheme, with information included in the publication scheme being routinely made available to anyone who consults it. A publication scheme is both a public commitment to make certain information available and a guide to how that information can be obtained.

The Freedom of Information Act applies to all recorded information held by English, Welsh, and Northern Irish public authorities, such as central government departments, local government, the police, the health service, the education service, and their related offices and agencies. The Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004 regulate right of access in Scotland along the same guidelines.

The rights conferred by the Freedom of Information Act may be exercised by anyone, including, but not restricted to, people living abroad, non-UK citizens, journalists, political parties, lobby groups, and commercial organizations. Exemptions where the public interest applies are (qualified exemptions):

- Information intended for future publication.
- National security.
- Defense.
- International relations.
- Relations within the United Kingdom.
- The economy.
- Investigations and proceedings conducted by public authorities.
- Law enforcement.
- Audit functions.
- Formulation of government policy and the like.
- Prejudice to effective conduct of public affairs (except information held by the House of Commons or the House of Lords).
- Communications with Her Majesty and so on and honors.
- Health and safety.
- Environmental information, as this can be accessed through the environmental information regulations.
- Personal information. People cannot access personal data about themselves under the Freedom of Information Act, as there is already access to such information under the Data Protection Act of 1998. Personal data about other people cannot be released if to do so would breach the Data Protection Act.
- Legal professional privilege.
- Commercial interests.

On February 2, 2005, *The Independent* was reporting that: "of the 70 inquiries made by *The Independent* only 10 have been successful. Almost half were turned down flat; the remainder are still awaiting reply. In two of the

replies the Government conceded that it had breached its own legislation by failing to meet the deadline of 20 working days that expired yesterday. Ministers also admitted they had no idea how many of the 362 requests made on the first day the legislation came into force had been answered." However, after a year of enforcement of the legislation, the impact on public agencies has been significant; in fact, a survey published by the Information Commissioner in January 2006 indicated that 66 percent of respondents had a very clear understanding, 36 percent reckoned FOI is a very good thing, 45 percent reckoned that it is a fairly good thing, 35 percent think that FOI increases openness and transparency, and 27 percent think that it forced agencies to improve records management.

36.3 CONCLUSIONS

Government executives who need to comply with FOI legislation will require tools that enable them to capture, archive, retrieve, and publish information rapidly while respecting privacy.

Historically the flow of documents between government agencies and constituents was paper-based, but the advent of e-government will generate a large amount of electronic records, which cannot be dealt with in the traditional way. Officials also will have to digitize existing paper documents to build comprehensive archives that enable a transparent and accountable view of all operations. Besides enabling compliance with transparency and privacy regulations, the design and development of electronic record and document management (ERDM) systems will eventually become the backbone of more responsive and efficient service delivery:

- Services will be delivered with higher responsiveness—citizens' requests must be input in case management/work flow systems, so that documents seamlessly go through all interested offices with no need for multiple queues.
- Back-office processes costs will be reduced—elimination of paperwork and reduction of duplications and correction of mistakes will reduce expenses.

Technology in itself will not be enough to ensure the compliance with regulations and a more responsive handling of documents. Bureaucracy/management changes will be required to support the implementation of technology solutions: definition of who is responsible for overall archiving management; definition of different levels of authorization to access, change, and publish documents; definition of type and number of backups; definition of cycle times to respond to internal and external requests for access to information; and so on.

References

Centro Nazionale per l'Informatica nella Pubblica Amministrazione (www.cnipa.gov.it).
German Federal Government (www.bund.de).
Legifrance (www.legifrance.gouv.fr).
Ministerio de Administraciones Publicas (www.map.es).
Ministero Riforme e Innovazioni nella Pubblica Amministrazione (www.innovazionepa.it).
UK Information Commissioner (www.ico.gov.uk).

CHAPTER 37

RETAIL

Ivano Ortis

37.1 INTRODUCTION

This chapter highlights the major retail-specific regulations, while providing future perspectives of the impact on processes and technology that are required to tackle present and future compliance dynamics. General accounting and enterprise principles such as labor legislations are out of the chapter's scope, although they apply to retail enterprises as well.

Retail organizations continue to be challenged by regulations compliancy and by the uncertainty about future regulatory changes. Rapid social trends, developments, and changes in government are posing additional complexities, thus requiring companies to develop a holistic approach to regulations and society evolution. In the retail industry, compliance is driven by government bodies, but, as in other industries, it is also market-generated. In addition, the increasing complexity of elongated global retail supply chains—better described in today's environment as "supply networks"—poses some additional challenges on identifying the responsibility of each party in the value network. As an example, food manufacturers, retailers, hotels, and restaurants are facing increasing social challenges such as an augmentation in the rate of obesity in many developed countries. The EU Commission is demanding that the European food industry stop advertising unhealthy food to children. Recently, the British Hearth Foundation launched in the UK a poster campaign to make especially children and teenagers think about what they are eating. In turn, food track and trace continues to be

a top priority that must be addressed coherently by all supply network partners, due to new potential health emergencies that must be kept under strict control.

Despite recent advancements, retail organizations are still showing a lack of smooth documentation policies and related processes. As an example, IDC Manufacturing Insights conducted in September 2006 a survey among 40 lines of business executives in the Western European retail and wholesale industry. Only 13 percent of respondents reported a complete definition of business processes into their organizations, while the majority of interviewees reported either partial documentation levels or no formal definition/documentation of business processes. As a result, most of retail companies in Europe will first need to get the basics right in order to flexibly manage compliance requirements and take full advantage of supporting technologies.

While many retailers, especially smaller organizations, continue to perceive the cost of compliance as a barrier to profitable growth, an increasing number of companies admit that some factors would encourage compliance; for instance, environmental health and safety regulations may improve their image in respect to consumers who particularly care about a better environment, or food traceability may dramatically improve the visibility over the supply chain, delivering better efficiency and customer service.

Retail business dynamics are also shaping new operative models requiring organizations to further extend regulatory compliance in areas that were traditionally out of their scope. An outstanding example is the strong growth of private labels or retail-owned consumer brands, which is evident on a worldwide level and particularly strong in Europe. As a result, it is crucial for retail organizations not only to ensure quality monitoring of branded products suppliers, but also to assess the impact of regulations that used to apply to consumer product manufacturers only.

37.2 COMPLIANCE IN THE RETAIL INDUSTRY

Compliance in the retail industry can be summarized:

- *Consumer safety*, encompassing, but not limited to, issues such as health and food safety, labeling of food and cosmetics, misleading advertising, and product safety (as an example, toys and hygiene)
- *Environmental issues*, as an example, recycling of used materials
- *Data and payment transactions*, including consumer data protection (e.g., privacy) and e-commerce laws

The major bodies involved in retail legislation around the globe are:

- The European Commission and its member states' governments, which are normally allowed to some degree of freedom in the initial adoption of regulations issued via EU decisions and recommendations, but then usually are required to harmonize local legislation to community-wide rules. The

European Food Safety Authority was established in 2002 to provide scientific advice and scientific and technical support in all areas impacting on food safety. It constitutes an independent source of information on all matters in this field, aiming to ensure that the general public is kept informed.

- In the United States, the Food and Drug Administration (FDA), its Center for Food Safety and Applied Nutrition (CFSAN), and the Federal Trade Commission for the consumer are the principal regulatory bodies for the retail sector. The U.S. Consumer Product Safety Commission was specifically designated to provide regulations, laws, and information by product category for manufacturers, importers, distributors, and retailers. In addition, the Alcohol and Tobacco Tax and Trade Bureau—part of the U.S. Department of the Treasury—provides the regulatory framework specific to the alcohol and tobacco industry.
- In Asia, the regulatory framework is rather fragmented across multiple country legislations. However, the disparate legislations tend to focus on the same set of issues that are raised in Europe and North America.
- The World Trade Organization (WTO) is the principal institution governing the flows of goods on a worldwide level, acting in close collaboration with European, North American, and Asia-Pacific bodies. Trading legislations such as antidumping and customs measures, mostly applicable to import and export of goods, have been excluded from the present analysis, as they usually impact mainly manufacturers, wholesale distributors, and their logistics partners. It is, however, the responsibility of retail organizations to ensure that appropriate codes of conduct are followed by their suppliers in respect of regional and local regulations, spanning from trading principles to labor and ethical principles. Therefore, retailers are required to maintain accurate information related to supplier transactions and actual flows of goods into their distribution centers, warehouses, and store back rooms or inventories, so as to ensure that audits can be performed either on accountability (e.g., order processing, duties, and taxation) or on product quality monitoring processes.
- The U.S. government defines the regulations upon which new retail stores can be opened, similarly to what happens on a country level in Europe and Asia. As an example, U.S. stores that sell food for home preparation and consumption must meet either of the following criteria:
    - The store offers for sale, on a continuous basis, at least three varieties of qualifying foods in each of the following four staple food groups, with perishable foods in at least two of the categories (the categories are meat, poultry or fish, bread or cereal, vegetables or fruits, dairy products), or
    - More than 50 percent of the total dollar amount of all goods (food, nonfood, gas, and services) sold in the store must be from the sale of eligible staple foods.

37.3 CONSUMER SAFETY

On a global level, governments and regulatory bodies have focused on providing all necessary information to consumers related to the products that are available on the market. Labeling is the more traditional element of this vital development, and comprises a separate set of regulations, depending on the product category (as an example, the labeling of textile products falls under 96/74/EC in Europe and under the Fair Packaging and Labeling Act 15 U.S.C. §§ 1451–1461 in the United States for all consumer products except food, with separate rules applicable to different types of goods).

Similarly, directive 2000/13/EC of the European Parliament specifies European laws relating to the labeling, presentation, and advertising of foodstuffs for sale to the ultimate consumer. In summary, the directive applies to prepackaged foodstuffs to be delivered to the final consumer or to restaurants, hospitals, canteens, and other similar mass caterers, while it does not apply to products intended for export outside the European Community. In short, the labeling, presentation, and advertising of foodstuffs in Europe must comply with compulsory labeling particulars:

- The labeling of foodstuffs must include the name under which the product is sold, list of ingredients, quantity of ingredients, or categories of ingredients expressed as percentages, including information related to allergens (Directive 2003/89/EC).
- Foods containing meat are subject to directive 2001/101/EC, which imposes specifications of net quantity and minimum durability.
- In addition, compulsory labeling principles apply to highly perishable foodstuffs, such as use-by date, special conditions for keeping and use, and name or business name and address of the manufacturer or packager or of a vendor.

In the United States the FDA, the first body that actually imposed that food and beverage products' labels include nutritional information as well, issued a similar set of regulations. In addition, the FDA established the Hazard Analysis and Critical Control Point (HACCP) for the seafood industry in 1995 and for the juice industry in a final rule released in 2001. In parallel, the U.S. Department of Agriculture has established HACCP for meat and poultry processing plants as well (USDA regulates meat and poultry, FDA all other foodstuffs). The FDA is now considering further developments to the current regulations that would establish HACCP as the food safety standard throughout other areas of the food industry, including both domestic and imported food products. In essence, HACCP involves seven principles:

1. Analyze hazards.
2. Identify critical control points in a food's production—"from its raw state through processing and shipping to consumption by the consumer"—at which the potential hazard can be controlled or eliminated.

3. Establish preventive measures with critical limits for each control point (as an example, cooking temperature and time).
4. Establish procedures to monitor the critical control points.
5. Establish corrective actions to be taken when monitoring shows that a critical limit has not been met.
6. Establish procedures to verify that the system is working properly.
7. Establish effective record keeping to document the HACCP system.

In addition, food safety principles are requiring compliance with a set of hygiene provisions. Similar to the U.S. regulations, the European legislation enforces member states to encourage the development of national guides to good practice by food business operators, including guidance on compliance with the general rules of hygiene (recently revised in regulation N. 852/2004) and to the HACCP principles. In essence, all food business operators "shall ensure that all stages for which they are responsible, from primary production up to and including the offering for sale or supply of foodstuffs to the final consumer, are carried out in a hygienic way in accordance with the regulation" in force. In practice, retailers are required to comply with this mandate during transport, handling, and storage of food.

Misleading advertising is one area where possibly all of the regulatory bodies throughout the world are currently enforcing the actual legislation. The Federal Trade Commission in the United States enforces such provisions, while the European Commission issued Directive 84/450/EEC to control misleading advertising in the interests of consumers, competitors, and the general public. In order to determine whether advertising is misleading in nature, factors such as the characteristics of the goods or services, the price, the conditions governing the supply of the goods or the provision of services, and the nature, qualities, and rights of the advertiser are usually taken into account.

It is also worth noticing that only in recent times have some European countries like Italy allowed for comparative advertising, which, on a European Community level, is regulated by EU Directive 97/55/EC. In essence, comparative advertising is permitted if the following conditions are met:

- It is not misleading.
- It compares goods or services meeting the same needs or intended for the same purpose.
- It objectively compares one or more material, relevant, verifiable, and representative features of those goods or services, which may include price.
- It does not create confusion in the marketplace between the advertiser and a competitor.
- It does not discredit or denigrate the trademarks, trade names, or other distinguishing signs of a competitor.
- For products with designation of origin, it relates to products with the same designation.

- It does not take unfair advantage of the trademark or other distinguishing sign of a competitor.
- It does not present goods or services as imitations or replicas of goods or services bearing a protected trademark or trade name.

Consumer associations and local European governments are particularly active in monitoring with respect to advertising principles, leading retail companies to litigation risk and to potential major costs associated with new marketing campaigns that are found to be misleading—not to mention the potential sales losses deriving from missing promotion-to-market objectives.

One related area, where the European Parliament recently issued a new directive aiming to harmonize different legislations across its member states, concerns unfair business-to-consumer commercial practices. Directive 2005/29/EC establishes a single common and general ban on unfair commercial practices that distort consumers' economic behavior. In essence, a commercial practice is unfair in the European Union if it is "contrary to the requirements of professional diligence, and if it materially distorts the economic behavior of consumers." The Directive makes a distinction between two types of unfair practice, those that are misleading and those that are aggressive.

(a) FOOD TRACK AND TRACE. The introduction of the new EU food regulation No. 178/2002 relates to all stages of production, processing, and distribution. The regulation introduced also the European Food Authority and defined both general and emergency provisions. The law essentially aims to prevent fraudulent or deceptive practices in the food trade that result in misleading information to the final consumer. The new regulation EC (R) 178/2002 took effect in January 2005, and requires all food and feed business operators to have in place systems and procedures that allow complete tracking and traceability of products throughout the supply chain.

As a result, "track and trace" capabilities will enable heightened food safety and product identity in the global marketplace while allowing for free movement in the Community of food and feed manufactured. The European regulation is affecting not only retail trade, wholesale trade, and food manufacturing, but also the HoReCa sector, which includes hotels, restaurants, bars, and catering service providers. The major responsibilities for food business operators are:

- Initiate urgent procedures to withdraw from the market any food that is considered not to be in compliance with food safety requirements, and accordingly inform the competent authorities. In the eventuality that the product may have reached the consumer, "the operator shall effectively and accurately inform the consumers of the reason for its withdrawal, and if necessary, recall from consumers products already supplied to them when other measures are not sufficient to achieve a high level of health protection."

- If retailers do not affect the packaging, labeling, and safety of the food, the requirement is limited to its respective activities—mostly limiting actions to initiate the recall procedure and sharing with relevant authorities and supply chain partners information necessary to trace a food.
- In the case of a batch, lot, or consignment of feed that may pose health risks, manufacturers and distributors are required to destroy the feed, and retailers shall cooperate in the action taken by relevant supply chain partners.

In addition, EU regulations require that all genetically modified organism (GMO) food products are labeled as GMO and that the product is traceable throughout the food chain (Regulation 1830/2003).

Therefore, those regulations, along with consumers' health concerns, are providing incentives for technology companies to provide pedigree solutions, as in the following example:

- The European Egg Consortium (EEC) and the METRO Group implemented in 2006 a central Online Service–Food Safety (OS-FS) system for backtracking eggs. The partners' objective was to create a transparent and real-time supply chain in the food industry through all stages from the feed producer and the egg farm to the retail store and the consumer. German initiatives such as the Product Liability Law and the Consumer Information Law as well as the American Bioterrorism Preparedness Act protect consumers and affect the entire supply chain in the food industry. Even before this, the EEC checked about 25 billion eggs annually under the labels of the Association for Controlled Animal Keeping and the Egg Products Association. The system includes the Online Service–Content Services (OS-CS) for the food industry. OS-CS collects and provides employee- and client-specific information for certain foods. These are made available to clients, the sales personnel, quality management in wholesale and, in the future, also to consumers at home. The food retailers will use this detailed information to offer their clients decision-making criteria for buying.

(b) GENERAL PRODUCT SAFETY REQUIREMENT. Directive 2001/95/EC of the European Parliament imposes a general safety requirement on any product put on the market for consumers, including products that provide a service and excluding secondhand products that have antique value or that need to be repaired. The European Union has introduced a rapid alert system (RAPEX) for products that pose a serious risk, and provisions for products to be withdrawn from the market if they are likely to put the health and safety of consumers at risk (as previously seen, food but also drugs are covered by other intervention systems). While mainly impacting consumer product manufacturers and distributors, requiring those companies to supply products that comply with the general safety requirement, monitor safety levels, ensure product traceability, perform product recalls, and inform accordingly both consumers and the competent authorities, it is important for

retailers not to underestimate the operational impact associated with product recalls and potential image losses. The latter factor assumed in recent times an even stronger emphasis due to the increased brand value of retailers versus consumer product goods that has occurred in the past ten years. Therefore, adequate suppliers' quality monitoring procedures should always be performed and documented by retail companies to counteract the effect of potential indirect risks.

A similar regulatory framework is in force in the United States through the Code of Federal Regulations (as an example, CFR section 7.3 g for cosmetics). The FDA strongly recommends that firms become familiar with the complete guidelines, including the components of a recall strategy, defined in 21 CFR Part 7. The recall strategy essentially involves the following key steps:

- FDA can request that a firm recall a product, including cosmetics, although these products are falling outside the scope of its authority.
- FDA monitors the progress of a recall by reviewing status reports maintained by manufacturers and by conducting audit checks at wholesale or retail customers to verify the recall's effectiveness.
- FDA may require public notification and assure that either FDA or the firm issues the public notification.
- FDA develops a recommended strategy for each recall or reviews and comments recall strategies developed directly by the firm owning the product.
- FDA makes sure that the product is destroyed or suitably reconditioned.

One of the most effective strategies to minimize the burden of product recalls is to prevent product adulteration and misbranding. As a result, supporting technologies such as radio-frequency identification (RFID) can effectively enable stronger mechanisms for ensuring product authenticity to all partners in the value chain and to consumers alike. But in case a recall does become necessary, companies can minimize the damage by being prepared in advance, as an example by maintaining a contingency plan for initiating a recall in accordance with the recall regulations, assigning production lot or batch numbers—although not required by law on certain products such as cosmetics in the United States—and by maintaining accurate distribution records exceeding the shelf life and expected use of the product to facilitate location of products being recalled.

Specific measures are defined for other product categories that may pose health risks, as in the case of toys (in Europe, regulated by decision 1999/815/EC). As an example, a recent report published by the Italian trade commission indicated in toys the product category with the highest number of products not found to be compliant with applicable regulations during 2006.

37.4 ENVIRONMENT: RECYCLING

Environmental protection measurers apply to retailers as well as to other asset-industry-intensive sectors, although regional differences are evident in the

provisions set for limiting energy consumption, ensuring water protection, and enabling more efficient waste management procedures. For example, U.S. government regulations extend also to a different cluster of issues, related to retailers' conduct on waste management of lamps (40 CFR 273.5 and 273.13 d).

Recycling is one environment-related area that is very specific to the retail industry. Strong focus is now on enhancing the recycling process—which is also driving demand for reverse vending machines due to European and German packaging directives. As an example, in light of the new German deposit regulation for cans as of 2006, self-service systems that accept one-way containers and refund the deposit are becoming increasingly important. Aldi recently ordered 2,500 reverse vending machines to handle one-way containers at the company's stores.

In more detail, the EU Packaging Directive says that member states must introduce systems for the return and/or collection of used packaging to attain the following targets:

- June 30, 2001: Between 50 and 65 percent by weight of packaging waste are recovered or incinerated at waste incineration plants with energy recovery.
- June 30, 2001: Between 25 and 45 percent by weight of the totality of packaging materials contained in packaging waste are recycled (with a minimum of 15 percent by weight for each packaging material).
- December 31, 2008: 60 percent as a minimum by weight of packaging waste will be recovered or incinerated at waste incineration plants with energy recovery.
- December 31, 2008: Between 55 and 80 percent by weight of packaging waste will be recycled.
- December 31, 2008: recycling targets for materials contained in packaging waste must be attained—60 percent by weight for glass, 60 percent by weight for paper and board, 50 percent by weight for metals, 22.5 percent by weight for plastics, and 15 percent by weight for wood.

But there are additional regulations directed to manufacturers that require some level of compliance for retailers. As an example, the Waste Electrical and Electronic Equipment directive (WEEE) requires manufacturers to pay for the recovery of used products. The EU strictly limits the use of toxic chemicals in electronic products and requires high-tech manufacturers to pay for collecting and recycling used goods. As of August 2005, manufacturing producers are required to achieve a series of demanding recycling and recovery targets for different categories of appliances. This clearly generates a supplier mandate for retailers, requiring intervention especially in the area of reverse logistics and supply chains more generally. Similarly, effective as of July 2006, the Reduction of Hazardous Substances (RoHS) directive bans the use of six chemicals, including lead, cadmium, mercury, and chromium-6, in almost all electronics products,

with the exception of military and medical systems as well as some telecommunications products. Once again, retail companies must collaborate with their suppliers, especially when bad events occur and responses need to be made to identify inventories of banned products and consumers potentially at risk.

37.5 DATA AND PAYMENT TRANSACTIONS

The Data Protection Directive establishes criteria for the protection of personal information across the European Union. Designed to enable the free movement of data while still protecting privacy, the directive mandates standards for the collection, storage, use, and disclosure of personal data, with especially stringent rules in place for the processing of sensitive data (such as information on health, ethnic/racial origin, political affiliation, etc.). The general data protection principles apply to all organizations, but additional measures need to be undertaken by organizations in the health care, telecommunications, finance, and human resources sectors.

These requirements are essentially driving investments in identity and access management security technologies, document and record management solutions, data recovery, and backup systems.

Security of payment transactions is driven both by institutions—as an example, during 2006 new "chip and pin" regulations in the UK fueled investments in point of sale (PoS) systems—and financial partners like Visa. In fact, achieving compliance with the Payment Card Industry (PCI) Data Security Standard is driving the requirement of building and maintaining a secure network infrastructure as well as implementing strong access control measures.

One element that is rapidly evolving and very peculiar to the retail industry is the legal framework for electronic commerce or e-commerce. In the move toward the information society, governments across the world have recognized in a stable legal framework for e-commerce a key factor to increase the confidence of Internet shoppers, while harmonizing Internet services to the general retail principles currently in force.

The European Parliament issued in 2000 directive 2000/31/EC, which covers information society services between enterprises, services between enterprises and consumers, services provided free to the recipient and usually financed by advertising income, and services allowing online electronic transactions for the sale of goods and services. While the directive applies solely to service providers established in the European Union, retailers should be aware of the current regulatory framework so as to ensure the right Internet service provider (ISP) partner selection, assess liability when transmitting and handling personal information, and requirements when evaluating new business models. In summary, the directive specifies the following:

- Provisions for commercial communications and spamming.
- Provisions for contracts concluded electronically, supplementing previous provisions on electronic signatures and aimed at removing restrictions adopted by member states' regulations.

- Liability of Internet service providers, in general stating that intermediate parties providing infrastructure services such as hosting and storage cannot be held liable for the information transmitted. Therefore, the entity initiating such transmissions or collecting personal information is deemed liable for such provisions.

37.6 LOOKING AHEAD

Retailers have the unique opportunity to differentiate their offering and generate new revenue streams adding new product categories to their multichannel strategies.

Private-label growth in the United States will continue unabated, which will pressure consumer packaged goods (CPG) margins and revenues in North America. Interestingly, previous strongholds of all private labels such as Lidl in Europe are adding branded products within their stores. This signifies a slackening of demand for purely price-driven decisions by the consumer as well as relief for the CPG manufacturers. Organic and natural foods will have double-digit growth in the United States, with Wal-Mart and Safeway and others adding organics, and this trend is moving into even higher gear in the EU. As a result, both branded CPG manufacturers and retailers selling own-brand products must achieve end-to-end visibility within their supply networks, both to comply with "track and trace" regulations and to gain new levels of supply chain efficiencies and flexibilities. As an example, Asda in the UK improved in 2006 its due diligence capabilities for private labels by implementing new IT systems and collaborative applications with some of its key manufacturing suppliers, such as Greencore. This example demonstrates that it is actually possible to derive business benefits from compliance, by improving new product introduction and supply chain operational efficiencies to the benefit of both top-line and bottom-line results.

An additional area where retailers are experiencing strong growth opportunities is in the sales of services. While traditionally mostly oriented toward warranty extension services and more recently digital printing services, new trends are emerging in Europe and in the United States.

Some of the largest European retailers, including Carrefour, Auchan, and Tesco, are rapidly penetrating into the mobile prepaid business by acting as mobile virtual network operators (MVNOs). An MVNO operates in a similar way to a normal mobile network operator but does not typically own the infrastructure or have a radio frequency license. Instead, MVNOs work in agreement with a licensed mobile operator that does own a physical network. This signifies that the applicable regulatory framework for retail organizations may extend in the future in line with the development of new business strategies, in turn requiring retailers to carefully assess the impact of changing regulations in the evaluation of new business models (as an example, in some European countries the current debate on the unfairness of fixed recharge fees for prepaid mobile services may lead to new regulations in the coming months).

In turn, Wal-Mart launched in February 2007 the beta version of its video download store, offering movies and TV programs on PC and portable devices. Wal-Mart is using Windows Media Digital Right Management (DRM) for this service and has been a part of the PlaysForSure group, which has been declining in popularity on the music side since Microsoft's announcement of Zune last year.

RFID and sensor networks are no longer perceived as emerging technologies, since an increasing number of advanced companies across the consumer products value network are proving the business benefits that can be achieved.

Environmental sustainability calls for both retailers and CPG companies to continue seeking and using organic materials for complete biodegradability of packaging, as landfills become less accessible and more costly to consumers. Product life cycle management (PLM) and waste management solutions will be used even more substantially to effectively manage and execute on these changes.

In conclusion, will retailers derive true business benefits from compliance? Clearly not all regulations may turn in immediate or long-term advantages, but at least we can identify, in the combination of track and trace and point of sale real-time data exchanges, real opportunities for retailers in their journey toward becoming more responsive, demand-driven, consumer-centric organizations. This fundamental process essentially involves four major steps:

Step 1. Clean and standardize item master data, implementing master data management addressing the minimum set of requirements and in addition the needs of different departments such as procurement, merchandise management, and sales.

Step 2. Enable supply chain and procurement efficiencies, by exchanging information with all suppliers in a single standard way. Global Data Synchronization Network usage will accelerate, enabling global access to standard data pools. In addition, achieving optimized supply chain management, execution, planning, and visibility will also increase, with a key emphasis on collaborative supply chain work flows. Global standards are now available, as defined by GS1 and EPCglobal.

Step 3. Ensure alignment and real-time flow of information toward marketing, sales, and corporate management, in order to optimize promotion planning and execution, revenue management, and business performance management capabilities. Product information management and merchandize management solutions will constitute the vital bridge between the supply side and the demand side, also to safeguard the due diligence process. Forecasting consumer demand—apart from seasonal and sale assortments where prediction accuracy is usually greater—will remain as the trickiest task to accomplish and will require advanced tailored applications.

Step 4. Ensure front-end to back-end integration (i.e., seamless flow of product information across store applications, PoS systems, mobile devices, information kiosks, electronic shelf labels, e-commerce platforms, and then back to enterprise systems) to close the loop enabling responsive retailing operations and improved business performance management capabilities.

References

http://eur-lex.europa.eu/en/index.htm.

The impact of regulatory compliance on Western European SMBs. 2005, *IDC* (April), Doc #MM51N.

U.S. Food and Drug Administration—www.fda.gov/.

Worldwide CPG/retail 2007 top 10 predictions. 2007. *IDC Manufacturing Insights (January), Doc #MI205042.*

www.europa.eu/scadplus/scad_en.htm.

www.wto.org/.

CHAPTER 38

SUPPLY CHAIN COMPLIANCE

Michael F. Cox

38.1 INTRODUCTION

Rather than attempt to provide specific references to hundreds of regulatory and guidance documents, the focus here is on best practices that will help any firm steer clear of ethical and compliance issues. The practices are more appropriate for firms of some size—large enough to be organized and staffed by function. Businesses that will benefit most are those where technical work is separated from administrative work, and divided into functions such as selling, processing orders, procuring goods and services, and so on. Very small owner-operator businesses are likely to be frustrated and daunted by the details, but the overarching business control principles are sound and broadly applicable. All business owners are encouraged to consult with a specialist or lawyer when dealing with issues of uncertain compliance requirements.

Many define *supply chain management* as tactical purchasing and logistics alone,[1] often referred to as "procurement." Ask someone about legal compliance for procurement, and two issues will inevitably rise to the top: (1) contract law and (2) uniform commercial code.[2] These are important and essential issues for purchasing operations, and will be touched on here, but hardly address the topic of compliance for integrated supply chain management. Laws to regulate business both financially and socially intersect largely with supply chain management in any organization, because, in its broadest sense, supply chain management touches all aspects of company operations.

According to Burt et al.,[3] supply chain management can positively impact the firm's bottom line more than any other business function, because supply systems include all internal functions, plus all external suppliers involved in the identification, fulfillment, and ongoing support of needs for materials, equipment, and services. With this more expansive definition, few company functions figure so prominently in the success of a company. Without an effective supply chain, a business is at a serious disadvantage. It is this significance that has propelled aspects of supply chain management to the front of many of the hard and soft laws designed to regulate business operations. A casual thumbing through *The Manager's Guide to Compliance*[4] leaves one hard-pressed to not see supply chain as a prominent concern.

The key to successful compliance for supply chain management is to ensure that there are clear roles and responsibilities defined for each step in the process. Adherence to commercial law, contract, and ethical standards of business conduct are prime concerns. Separation of duty, process rigor, and unfailing management oversight are key concepts of adequate controls. These concepts are reinforced in the long-standing and evolving guidelines of the Financial Accounting Standards Board,[5] as well as recent laws promulgated in response to corporate scandals, such as Section 404 of the Sarbanes-Oxley Act[6] for publicly held companies registered with the U.S. Securities and Exchange Commission, and similar international accounting and business control principles and rules.[7]

38.2 SEPARATION OF DUTY

In firms large enough to support a functional organization, professional buyers should act as purchasing agents. In publicly traded firms, this is a particular concern for the prevention of fraud and theft. Only qualified buyers should be contacting suppliers for procurement negotiation, unless an exception is approved by an appropriate level of business management. Requesting purchasing services, and the act of procurement, should be separated from receiving the item, processing supplier invoices, and making payments to the suppliers. The person engaging the supplier to negotiate and make a financial purchase obligation should not be the person who needs the item (the requestor), nor the person processing and paying the supplier invoice. This degree of separation may not be practicable in a small, individually owned business. The critical thing is to ensure separation

of commitments and payments, and complete management oversight of spending activities at all levels of the firm and for all types of spending.

If the firm uses electronic software systems for controlling aspects of the procurement to payment process, direct editing capability for associated master data in the software system must be restricted to authorized personnel only. Only an authorized job function such as a buyer should be able to create or edit purchase order (PO) documents released to suppliers. Management must keep the system access authorities up to date as employees come and go, tasking the designated system administrators to periodically review and remove inactive names. The system, as well as the process for manual orders, should not allow the name of the buyer and the requestor (the person who asks for and will use the procured good or service) to be the same.

38.3 SELECTION OF SUPPLIERS

For reasons of financial control, legal compliance, and business management quality, the act of selecting new suppliers must be carefully controlled. Existing suppliers should be reused where possible. Firms should have written guidelines for selecting suppliers, and the guidelines should preserve the separations of duty and include management review and approval of the commitments. In firms large enough to be functionally organized, the process for engaging and negotiating terms and financial commitments with suppliers should be in the hands of qualified sourcing professionals. The rigor of the selection process should be commensurate with the strategic importance of the item and the desired results.

At a minimum, selection considers price competitiveness and the supplier's ability to meet the requirements. Leading firms use a framework or checklist approach to assuring that all relevant aspects of the desired results are addressed. There should be independent management approval for sole and single-source suppliers. Selection policies and guidelines should be communicated to all involved departments, and the selection process should be tailored to the potential impact on operations and customers in order to meet the principles of a quality business management system. Supplier selection should include a check against lists of restricted parties, such as the U.S. Blocked Persons, Denied Persons, Entity, and Debarred Parties lists.[8] There may be literally dozens of such lists that could apply to an item. Records of the supplier selection criteria, evaluation, and results should be retained for at least the period of time that the relationship is active, plus the duration of any associated contractual commitments, such as warranty terms.

Supplier relationships must conform to ethical standards of business conduct. Section 406 of the Sarbanes-Oxley Act requires that the firm disclose whether it has a Code of Ethics for its senior executive management or explain why the firm has not adopted such a code.[9] In addition, there are laws that govern supplier selection in certain international jurisdictions, such as the U.S. Foreign

Corrupt Practices Act of 1977.[10] Employees with supplier selection management responsibilities should be trained in these and all relevant aspects of the firm's standards of business conduct. Nonconformities inside the firm and in its dealings with suppliers should be quickly corrected upon discovery, with appropriate notifications to management. Corrective action records should be retained for an appropriate period of time as determined with legal counsel.

38.4 RISK AND BUSINESS CONTINUITY MANAGEMENT

Suppliers that could have a materially significant impact on the firm's operations should be checked for financial risk and business stability before the first order is placed. There should be an ongoing process for monitoring financial conditions at these suppliers. Larger firms may have a risk management department that drives reviews of the risk controls and contingency plans for significant strategic suppliers. Besides being a good business practice, supply chain risk assessment and management may be required by third parties that have a stake in the business and the risk, such as insurers and lending institutions.

Suppliers will do well to have business continuity and risk contingency plans that are available upon request. There are many consultants in the marketplace that can expedite the production of such plans, but the firm will need to ensure the plans are made operational. Significant relationships should include periodic confirmation of the continued conformance and validity of the outsourcing objectives and arrangements. In companies registered with the U.S. Securities and Exchange Commission, unplanned events in the supply base that could materially change business financials should be immediately discussed with a financial officer to determine if reporting requirements apply, including Sarbanes-Oxley Section 409.[11]

Supplier performance evaluation is a wise management technique that can improve the certainty of supply-base business continuity. The degree of evaluation is tailored to the nature of the relationship and the item, with strategic suppliers of critical items receiving the most attention. By their nature, however, evaluations are retrospective. The best practice is to develop performance measures that can be tracked in real time and over time, such as on-time delivery, and then use these to manage corrective and preventive actions for individual incidents, as well as information to feed into an overall performance scorecard. Reviews of the scorecard are best when they include a diagonal slice of management from both firms, from logistics up through executive management. Another way to mitigate risk is to try to control the addition of new suppliers, discussed earlier.

38.5 PAYMENTS

Basic principles of accounting require that payments be verified. Invoice verification procedures should be defined and assigned to responsible personnel, typically accounts payable. Procurement personnel, typically buyers, are responsible for ensuring that purchase order quantities, prices, and other relevant details

are entered accurately. Invoice holds caused by issues controlled by procurement should be tracked, minimized, and cleared in a timely manner. Returns and credits against invoices need to be tracked carefully. A proper credit should be entered on the books against the invoice received or paid.

If the firm uses standard payment types, care should be taken that any exception to a payment term is not applied to the wrong order or left in place for orders other than the one to have an exception. Many firms will choose a default or standard payment term for their orders, such as net 30 days. When doing so, one should not inadvertently lock out the significant discounts that can be obtained for prompt payment. It should also be recognized that commercial code and/or custom in different countries may require different payment terms. Sometimes the terms may be more prompt in exchange for a discount, such as 2 percent to 3 percent for net 14, else net 30. Some types of payments may be expedited as a rule of courtesy but not necessarily law, such as payments for customer refunds, utilities, donations, legal payments such as penalties and fees, and payments to manufacturing representatives.

Pricing for procured goods and services should be reviewed periodically, especially where there is variance between the purchase contract price and the invoice price. Discrepancies should be resolved in a timely manner. A particular matter of compliance with financial rules and principles is how to deal with price changes and the valuation of physical inventory. As a matter of good business management practice, supplier pricing should also be periodically evaluated to ensure it remains competitive. This includes recognizing that for some items there may be a significant learning curve. If the item can be produced more efficiently as time goes on, the price should decrease similarly.

38.6 ITEM AND SUPPLIER SETUP

Firms that use electronic procure-to-pay systems must ensure that system information is kept up to date with regard to changes. Employees must not manually work around the system. Every instance of working around the system, even under the rationale of acting first and updating the system later, must be discouraged and reprimanded when it occurs. When it is known that data in an electronic processing system is not complete and completely accurate, trust in the system is lost and disregard for the system spreads quickly. Purchasing information for transactions must be complete, accurate, and entered only once in the electronic processing system. Data should not be mastered in more than one system.

Procedures should be established and followed for data entry, assignment to transactions, and changes. The creation of duplicate records in the system in order to force an exception to system rules and capabilities must also be discouraged and corrected. Transactions that are rejected due to faulty data must be isolated, analyzed, and corrected in a timely manner. Supplier and item master data setups and changes should be restricted to authorized purchasing personnel. Prior to release, master data revisions should be reviewed and approved by appropriate

managers from the affected life cycle functions, such as marketing, engineering, operations, and support. Sourcing rules and assignment sets should be defined and maintained so that supplier-to-item relationships are established completely, accurately, and one time.

38.7 CONTRACTS AND PURCHASE ORDERS

The term *contract* is used here to mean the entire purchase order or agreement, including the order itself, the legal terms and conditions, and any supplemental information such as work descriptions, specifications, and drawings. As always, one must recognize that a contract is a historical record of mutual understandings and agreements, but a supplier relationship is dynamic and changing every day. The most innovative contract systems recognize and easily accommodate the less formal day-to-day communications and agreements typical of a dynamic relationship.

Only authorized workers should be able to enter into and modify purchase orders and contracts. New contracts should be reviewed by legal counsel competent in the matter. Too often people take an old contract and attempt to update and use it without an adequate understanding of the principles of law that underlie the contract and whether they are applicable for the type of transaction and the country(ies) where the parties are located. After a contract is final, prepare a checklist of the terms and conditions that should not be changed without legal review. For smaller firms, outside counsel is an economic alternative to having a legal department in-house.

Purchase contracts need to be kept up to date, administered, and enforced. Negotiations with a supplier should not take place without immediate access to applicable contractual terms and specifications. There should be a policy regarding the standards of contract duration and renewal. There should be a decision regarding the types of purchasing records that need to be maintained, where, and for how long. Record retention decisions need to be based on consideration of factors such as accounting standards, tax and trade laws, and the business management standards of the company.

It is a good practice to maintain a template of purchase contracts based on the commercial law of the country where the firm is headquartered or incorporated. The standard terms may then be supplemented with any special terms that are required for unique issues associated with the item or service of exchange. If terms and conditions, including specifications, are issued at different times or at multiple levels (master, supplemental, order, etc.), it is important to state the order of precedence and to be sure that a conflict in any one area does not void the remaining contract.

Predefined controls and staff education are the keys to managing changes in contractual requirements. Employees responsible for following the rules of the contract need to be educated about the rules and the process for controlling changes. Changes should be approved by appropriate levels of management, based on the aggregate value of the relationship and not just the immediate transaction.

A best practice is to maintain a contract repository where a record of the legal review and approval of the contract and subsequent changes is maintained. The record includes approval by the appropriate level of management based on financial significance. If the firm is certified to a quality business management system standard, such as ISO 9001, the controls and records must be maintained.

Some companies set up secure "electronic rooms" where specifications and other work instructions are shared and mutually maintained in real time. These operate under blanket legal terms and conditions that typically remain fairly static over the life of the relationship. Other may rely on a structured service level agreement approach, where different preagreed terms and conditions come into play depending on the type of service selected. The important thing is that the parties do not agree to take an exception to binding legal terms and conditions without review by a legal professional and documentation of mutual acceptance of the change.

Purchase orders should have a corresponding requisition or management approval of any exception. Exceptions could be automatic releases under authorized blanket purchase orders and agreements, and urgent hotline manual orders authorized by management. In any case, purchase order records should be periodically reviewed by management in order to correct and prevent unauthorized exceptions. Any deviations from a rule should be isolated, analyzed, and corrected in a timely manner, including making sure only authorized persons engage in purchasing activities.

Where software systems are used, automated reports should be generated periodically in order to identify and review purchase requests and purchase order exceptions. Factors that should be included in the reports are requisitions auto-generated by rules of the software system, if any; incomplete purchase orders; purchase orders in reapproval status; past due orders; open orders, including aging; purchase orders not acknowledged; and purchase orders in expedite/push-out/cancel status.

When purchase orders are fully received or no longer needed, they should be closed. This is an administrative step that should be given adequate priority. One risk of not closing purchase orders in a timely manner, as well as completed line items within blanket purchase orders, is that a supplier of more than one item might be allowed to bill overruns for item one to the balance remaining for item two. This obscures the cost overrun for item one and distorts the total buy information for both items.

38.8 TRACKING AND REPORTING PURCHASE OBLIGATIONS

If the firm is public, material contingent liabilities must be disclosed. For firms registered with the U.S. Securities and Exchange Commission, the Sarbanes-Oxley Act restates and reinforces reporting principles. Sarbanes-Oxley tightens deadlines for notification, the range of potential obligations and liabilities that must be reported, and the penalties for nonconformance to the rules. The Sarbanes-Oxley Act lays out specific categories of reportable obligations and a reporting format.

According to Tarantino,[12] similar requirements are found in the Australian Stock Exchange's 10 Principles of Good Corporate Governance, Canada's Multi-Lateral Instruments 52-109 and 52-111, the United Kingdom's Turnbull Guidance and Combined Code, and the Organization for Economic Cooperation and Development (OECD)'s Principles of Good Corporate Governance.

Contractual (written or binding verbal) purchase obligations should be tracked by finance. Purchase obligations can be factual, an obligation to pay for services or goods already received, or contingent, an obligation to pay for something in the future upon the occurrence of a triggering event. Material commitments that can have a future impact on business if conditions change must be tracked and managed responsibly. According to Tarantino,[13] other important considerations are the 2004 Basel II Accord for the banking industry, Solvency II for the insurance industry, and the Graham-Leach-Bliley Financial Modernization Act of 1999 for the financial and insurance industries.

If the business has a separate finance department, as it should, obligations must be tracked, monitored, and reported to persons responsible for financial control. It is wise to establish written policies and procedures. All employees who could create or trigger an obligation must be trained in the control and reporting processes. Purchasing managers should ensure that they track the total amount of contractual purchasing commitments and liabilities on a quarterly basis, including off-balance-sheet obligations. These are obligations that are not normally accounted for in a profit-and-loss statement, such as a binding commitment to pay a supplier for loss of business or a commitment to buy back inventory if business orders fall off.

A best practice for dealing with purchase obligations is to use special software to capture, track, and report obligations to management. Many software systems for business financial management and planning have these capabilities, either built in or available as extensions of the software. In firms that do not use electronic systems for procurement management, the use of a contract summary sheet that details the potential liabilities is an acceptable approach. The sheets are forwarded to a responsible manager for analysis, reporting, and retention.

Be careful to capture, track, and report purchase obligations of all types, both the obligations of open orders as well as commitments that may not be noted in an order. Obligations should be incurred only by authorized personnel operating under management oversight. Obligations that do not involve goods and services at time of receipt (often called nonreceipt and nonorder purchase obligations) must be recorded completely and accurately. Be careful not to enforce obligation controls and reporting requirements in a way that encourages employees to break up transactions or similar acts to work around the controls.

38.9 ASSURANCE OF SUPPLY

Financial controls dictate that supply shortages that could materially impact operating results are actively tracked and evaluated to improve preventive actions.

Suppliers are responsible and held accountable for maintaining supply at the levels specified. Open orders are reviewed on a regular basis to identify supply that is past due and/or requires expediting to ensure that the good or service to be supplied is delivered on time. An effective process to assess supply chain business continuity risks (mentioned earlier) and the planning and scheduling considerations discussed later are the best defense against material shortages that result from practices within the buying company.

38.10 SUPPLY CHAIN PLANNING AND SCHEDULING

Supply planning and scheduling problems are a great financial risk to any firm and must be adequately controlled. In firms large enough to be functionally organized, there should be planners with responsibility for supply optimization. The planners should ensure accurate calculations and reserves through appropriate levels of review and management approval. Items with current period reserves that exceed a tolerance level should be reviewed by management and cost accounting. If the firm uses planning and scheduling software, tolerance limits should be properly configured to limit safety stock. If the planning parameters (min/max, etc.) of the system are periodically adjusted to mitigate potential inventory risks, the adjustments are based on sound scenario analysis.

If just-in-time (JIT) or other lean-inventory manufacturing processes are used,[14] materials purchasing processes should be periodically evaluated to reduce the impact of bottlenecks. In any firm converting materials to finished goods, the days of inventory supply on hand must be tracked to prevent both inventory shortages and excess inventory. In larger multinational firms, tracking should examine inventory positions within an individual product line, as well as across lines where materials are used across lines. Publicly traded firms registered with the U.S. Securities and Exchange Commission will need to meet the real-time reporting requirements of Section 409 of the Sarbanes-Oxley Act for material changes in inventory positions, as these affect financial reporting.[15]

Many firms at one time or another have disposed on excess and obsolete inventory, only to find out later that a different product line could have used the material. Another common problem is product lines competing against one another for constrained supply when they do not coordinate their different internal purchases from the same supplier. Adequate sales and operations demand planning and matching should be used to avoid negative impacts from changes in business conditions. The reasons for changes in demand should be recorded and considered in future planning, for continual improvement.

38.11 INVENTORY MANAGEMENT

The firm should have documented procedures for ongoing inventory control management. Inventory should be kept in the correct location and protected from theft and loss. Overall inventory scrap, excess, and disposition (sale, disposal, and returns) should be evaluated for excessive waste from time to time and

supported by financial accounting as necessary. Cost accounting should track inventory positions from quarter to quarter. Management approval authorities for inventory positions and changes should be classified by dollar thresholds and adhered to. Inventory provisions should be reviewed by a purchasing and financial manager.

There should be local processes and procedures for determining when to inspect received services and goods. Work procedures should be in place if inspection and/or other activities are needed to ensure the product meets the requirements. If the firm or its customers intend to perform verification at the supplier's site, the purchase contract or order should specify the verification arrangements and method of product release. Procedures should include ongoing loss-prevention processes for materials receiving, storing, processing, and disposition operations. The tolerance limits for goods received should be enabled and limits should be specified as per company policy. This is because accounting rules require some level of notification to the receiver when the quantity entered into the system during a receiving transaction is greater than the order quantity (expected receipt quantity).

There should be a process for the identification, tracking, and escalation of services and goods that do not conform to the firm's requirements. Corrective actions should be commensurate with the potential severity of the nonconformance. Nonconforming goods should be segregated and tracked to ensure accurate and timely returns, as well as financial credits in accordance with the order terms and conditions. A record of the nonconformance and corrective action should be retained in the local contract file for the supplier. If electronic procure-to-pay software is used, return transactions should be appropriately entered into the system, including authorization. The return process should ensure that financial accounting changes for the inventory return are accurate and timely, the original PO is active or reopened to capture the resulting credit, a credit memo is triggered, and the material is physically shipped to the authorized point of return.

Where physical goods are involved, amounts paid to suppliers for consigned buy/sell inventory price differences (due to market value fluctuations) should be reasonable and in accordance with contractual agreements. Management should establish thresholds for approval. Production and inventory price variances should be reviewed on a monthly basis by cost accounting, and significant variances should be investigated and resolved. Accounting should ensure that there are no zero-cost parts on bills of material in progress that could result in undervalued inventory. Accounting should work with procurement and planning to resolve any issues.

Third parties holding inventory on the firm's behalf should do so under written legal agreements that stipulate the liabilities for the inventory and the key management requirements (protection, delivery, etc.). Third parties holding inventory owned by the firm should provide written verification of quantity, value, and

loss-prevention processes. The third parties should also provide monthly reports that are shared with financial accounting as necessary to maintain book entries, especially as regards excess and obsolete (E&O) inventory.

Setups for contract manufacturing orders and the associated direct material transactions should be properly classified and recorded with respect to inventory arrangements (e.g., buy/sell, consigned, outside processing [OSP], or turnkey). The respective arrangements should be periodically reviewed (nominally annually) to ensure proper inventory reserves and accruals, if any. Liability for all materials, work-in-progress, and finished-goods inventory held by third parties on the firm's behalf should be tracked by the business on a monthly basis and communicated to the financial controllership. Supplier consigned inventory levels and any associated reserves should be periodically examined for reasonableness relative to historical usage.

Arrangements for inventory held by third parties should be examined by the financial controllership to determine the financial accounting method that meets financial guidance and controls, such as Generally Accepted Accounting Principles (GAAP) and/or Committee of Sponsopring Organizations (COSO). Encumbrances against supplier inventory (obligation to buy back, custom manufactured parts, held for the firm, etc.) should be disclosed to financial accounting. The firm must record inventory and associated liability at the time the firm takes ownership of inventory from the supplier. The ownership transfer must be controlled and accounted for financially.

Physical inventory cycle counts should be completed in accordance with financial requirements and applicable tax and trade law. There should be a set definition for tolerable discrepancies or local exceptions. Parameters for determining E&O inventory should be appropriate and not unduly lengthy. E&O inventory should be managed in accordance with financial requirements and applicable tax and trade law, including:

- E&O reviews by procurement, planning, and financial accounting for early identification and optimization of resulting issues (a best practice is quarterly reviews);
- timely and accurate valuation and recognition;
- timely disposition with evidence of sale or scrapping, with release of reserves justified by record of sale, disposal, or change in applicability of reserve standards;
- reserves, releases, and reporting in accordance with applicable accounting standards (GAAP, SAB 100, etc.) and tax reporting requirements. The inventory liability reporting process should include a detailed item-by-item cost-accounting review for third parties holding inventory encumbered or owned by the firm; and,
- E&O files sent to authorized personnel for review should be password protected.

38.12 PHYSICAL ASSET PROTECTION, INTELLECTUAL PROPERTY, AND CONFIDENTIALITY

In any purchase contract involving the transfer and use of physical property, as well as materials and items used to manufacture company products, there needs to be adequate provisions to assign responsibility for the control, protection, ownership, and ultimate disposition of the physical property. Liability for excess and obsolete inventory, whether raw materials, work in progress, or finished goods, is an area of particular focus. Especially risky from a financial compliance and enforcement standpoint for publicly held companies is the practice of removing inventory liability from the company books and disclosures by contractually transferring ownership to third parties. If the company imposes any restrictions on the control of the transferred inventory by the third party (encumbrances), the arrangement should be considered suspect.

Intellectual property (IP) is also an asset that requires careful management. The trademarks, patents, and copyrights of the firm must be protected to maintain clear ownership. Suppliers should not be allowed to use any of these items without an express written agreement. Without taking the time to define ownership of intellectual work product, a company might be surprised when a supplier refuses to hand over an intellectual work product, such as product design drawings and specifications.

Agreement provisions for both inventory and intellectual property controls should be reviewed by a purchasing manager and a financial expert. If nonstandard agreement terms are used for either issue, the language should be reviewed by a commercial attorney. It is also important to remember that the transfer of physical assets, as well as labor assistance, may trigger tax and trade reporting and payment obligations. Assist is discussed further in the next subsection (regarding logistics, tax, and trade).

Great care needs to be given to the issue of confidential information. Among technical professionals, there is a tendency to share freely in a collegial manner. It is important to establish a system that does not dampen beneficial collaboration, but makes it clear when an item of the exchange is proprietary and confidential. Typically, this is accomplished by adopting contract terms that prescribe degrees of confidentiality and control based on how exchanged information is marked. No property or sensitive intellectual information should be lent or transferred to and from the company without an applicable property control and/or nondisclosure contract. Items should be marked to show ownership, level of confidentiality, and for tracking. Personnel should track company-owned items, verify adequate protection in the hands of the other party, and ensure return upon request or upon termination of the supplier relationship.

An area of frequent abuse is the sharing of confidential pricing information. To prevent questionable practices, price nondisclosure requirements should be included in purchase agreements where price is not public information. The requirements should be binding to all individuals up and down the supply chain

who might be party to the confidential pricing. Access to negotiated prices should be limited as much as possible. Nondisclosure terms should be reviewed periodically to ensure adequacy based on the specific supplier relationship and work.

38.13 LOGISTICS, TAX, AND TRADE

Primary logistics compliance concerns for supply managers are ensuring the supply network has effective policies and procedures in place for tax and trade compliance. Export, customs, and dangerous goods controls are the primary concerns. All items crossing international borders must have a product classification prior to shipping, consisting of the applicable export, customs, and dangerous goods classifications. There are many regulations internationally that require some degree of notification, registration, and restriction of international shipments of certain chemicals and waste.

Larger firms typically integrate many of the logistics and trade restrictions into their purchasing processes; for example, reference to the U.S. ban on ozone-depleting substances is often found in purchase order terms and conditions. Controls should be in place to ensure that the proper freight terms are noted on purchase orders and are in accordance with the terms and conditions for the purchase order. The most common trade violations are failure to declare and making false or fraudulent statements. Customs agencies will have enforcement priorities by subject, such as item classification, and by industry, such as agriculture. Smaller firms may find it necessary to retain the services of a consultant in order to develop internal control processes for the many requirements, especially regulations regarding chemical and waste shipment.

Substantial time and energy are necessary to gain and retain logistics, tax, and trade regulatory expertise in-house. For this reason, many smaller businesses rely on outside experts such as international freight forwarders to help them in this area. There are also organizations to assist small businesses wishing to expand, such as the International Business Forum.[16] Many can be found through the Internet. National departments of trade, customs, or commerce are other good places to start when attempting to understand export and import controls. There are also many excellent service providers and software solutions for logistics, tax, and trade compliance.

Regardless of whether compliance is managed in-house or outsourced, a prudent supply chain manager will want to be assured that the supply-base network is effectively managing item classification, export and import licensing and data reporting, fee payments including brokerage fees, and adherence to restrictions such as restricted and excluded party lists. Leading companies typically use logistic service providers to receive goods at the supplier's dock or an in-country location and then handle classification and shipment to the final destination. In this way, the firm is able to maintain better control and to capitalize on the efficiencies of scale, standardization, and other cost savings opportunities. As an

example, the expansion of the European Union has benefited supply chain costs in that individual national tariff schedules were replaced by a harmonized schedule for member states.[17]

An international trade issue that requires careful training of personnel is when a customer of a supplier transfers assets and/or labor to the supplier at no cost and the transferred items are used to make goods that are shipped across international boundaries to the customer. This is called "assist." The invoice for the goods and services received by the customer must record the true value of the item for the purposes of customs reporting and applicable duties, if any. The assist value is added to the supplier's invoice price to calculate the transaction value. Assist rules are dictated by the World Trade Organization, Customs Valuation Code, and the customs valuation rules of most countries.[18]

The transaction value is the basis for customs valuation of items that are shipped across international borders. Other methods of valuation are allowed by law, but the transaction value is always the starting point. One way to avoid assist is to sell items to the supplier at fair market value rather than transfer them at no cost. The prudent manager will establish an assist policy to restrict transfers of firm-owned labor and property (assets and IP) to suppliers.

Free trade agreements, the networks established thereby, and the tax and tariff advantages must be considered by any supply chain manager doing business internationally. Many free trade organizations provide assistance with assessing the advantages of doing business within these networks as opposed to outside them. Keep in mind, however, that sometimes the cost of meeting the agreement rules on origin may be higher than the cost advantages offered.

A good example of a leading free trade organization is the Singapore Free Trade Agreement Network.[19] Similarly, the Closer Economic Partnership Arrangement (CEPA)[20] between Hong Kong and the Chinese mainland offers significant tariff advantages for Hong Kong companies. These are just a couple of examples of hundreds of opportunities available internationally. Economic and societal development benefits may also be found in organizations other than those expressly for trade. For example, the Association of Southeast Asian Nations[21] has many activities designed to promote and foster free trade.

In response to the terrorist attacks on the World Trade Center in New York, the U.S. Customs Service (now called Customs and Border Protection) established a program to increase the antiterrorism security of commercial shipments to the United States. Customs and Border Protection established an incentive program for business called the Customs-Trade Partnership Against Terrorism (C-TPAT). Companies that participate in the program have to demonstrate effective antiterrorism controls within their own facilities and over shipments to the United States originating from their international supply chain networks and customers. In return, the companies are given special designations to speed their shipments through Customs and Border Protection.

38.14 ANTICOMPETITIVE BEHAVIOR

In nations with well-developed commercial laws and practices, it is typically illegal to make deals to deliberately eliminate market competition. Information and publications regarding competitive commercial law and compliance are substantial. The Organization for Economic Cooperation and Development (OECD) publishes competitive law summaries for 23 countries online.[22] Information for other countries, including the United States, is generally available online. The EU's legislation, based primarily on Articles 81 and 82 of the Treaty of Rome, are also online.[23]

This area of law is very complex. There are entire journals dedicated to subjects of competitive regulation of commerce. Although details vary considerably, the general principle of the different laws and regulations is the same: the prevention of deals to exclude certain companies from doing business in certain areas or with others, and any other deal that can be alleged to be for the purpose of fixing prices or otherwise limiting free market competition. The deals can include bribes, fixing or manipulating prices, and agreements between firms to allocate market access (territorial and customer-based limits).

The key to understanding compliance responsibilities for supply managers is to understand that the majority of the compliance burden is on sellers, not buyers; for example, see United States Code[24] Title 15, Commerce and Trade, Chapter 1, Monopolies and Combinations in Restraint of Trade, Section 14, "Sale, etc., on agreement not to use goods of competitor." A buyer can be swept up nonetheless if it inadvertently or deliberately agrees to or asks a seller to exclude one or more of its competitors from access to the seller, or the buyer works with a seller to exclude one or more of the seller's competitors from doing business with the buyer.

The key to anticompetitive behavior is to maintain independence of all buying decisions and not to tie the choice of who to do business with to the requests or demands of a third party. The trouble lies in the fact that there are gray areas. Assess whether the action is or could be alleged to be an intentional exclusion of a company from market access. The compliance issue is the distinction between dealings for a good or service in which the buyer has complete freedom of choice and dealings that are specifically contrived to eliminate competition by limiting choice. A prudent supply manager will pay special attention to these areas.

38.15 QUALITY REQUIREMENTS FOR THE BUSINESS MANAGEMENT SYSTEM

Many businesses are registered or certified to a business quality management system, such as the ISO 9000 quality management system.[25] Impetus for quality management comes from the market. Firms recognize the value of a reputation for delivering services and goods that meet or exceed customer expectations. Due to the rapid growth of outsourcing as a business management practice, quality management systems are increasingly focused on supply chain management.

Today the focus is on the concept of controlling the outsourcing of an operation or item production in order to ensure the complete satisfaction of the ultimate customer.

For publicly traded companies, there are also mandatory requirements, such as those of the Sarbanes-Oxley Act. Tarantino[26] summarizes the requirements and key considerations of Section 404 of the Act, which calls for the creation and maintenance of viable internal controls to ensure effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. The SEC holds the company chief executive office and chief financial officer personally and criminally liable for the quality of the firm's controls. A supply chain manager would do well to integrate consideration of the SEC controls into the day-to-day business quality management systems.

Based on the work of Burt,[27] effective supply chain quality management starts with complete and appropriate requirement specifications before the first order is placed. Suppliers are selected based on having the necessary systems and capabilities to meet the requirements. Too many firms select the supplier and then negotiate the requirements in the belief that being too specific about the work will impede the supplier's ability to suggest innovations. This is a fallacy if the focuses on clearly defining the results it expects, but leaves the supplier freedom to propose innovative methods of fulfillment. Nonetheless, if the firm understands that there is a definite process that will yield the desired result with great success, it had best define the process in the requirements and then discuss any potential improvements the supplier might suggest.

Information tendered to the supplier during negotiations leading up to the initial order should describe the product to be purchased, including, where appropriate:

- Statement of work that defines the deliverables, milestones, pricing, payment, and billing requirements
- Requirements for qualifying and approving the procured services and/or goods, and the supplier processes, procedures, and equipment to produce it
- Qualification requirements for key personnel
- Management system aspects the supplier is expected to have, including quality, social responsibility, and the environment

When requirements are completely defined and an able supplier is on board, the next quality management issue is that of establishing performance objectives to motivate continual improvement and the controls to perform accordingly. There should be real-time monitoring of supplier performance and exercise of appropriate control. This occurs in the context of the "plan, do, check, act" method of management advanced by the business quality management systems.

For strategically significant suppliers, senior supply chain management should be involved in periodic reviews of the supplier's performance and

improvement objectives. Sourcing personnel should be trained in the general quality management system, in addition to being trained in the specific supplier quality management tasks that are assigned to them. There should be a record of the results of supplier performance evaluations and improvement actions arising from the evaluations. The record should demonstrate follow-through on the actions.

38.16 SUPPLY CHAIN ENVIRONMENTAL AND SOCIAL RESPONSIBILITY MANAGEMENT

Figuring prominently in the regulatory and governance schemes is an ever-growing principle that a business has some legal and moral obligations for its choice of firms with which does business. A company with underwriters, investors, and lenders is expected to make transparent all aspects of its outsourcing arrangements. With increasing visibility and size, a company will feel increasing pressure to ensure its suppliers are ethical and legally responsible firms. Not only this, but in some sectors, such as electrical and electronic equipment manufacturing, there is an increasing sentiment that a manufacturer should be responsible for its product throughout its entire life cycle. This is driven mainly by concerns about the ecological risks of chemical substances contained in the products, such as lead, chromium, cadmium, and brominated flame-retardant chemicals.

Beyond law, in the public court of opinion, a producer may be held responsible for its suppliers and suffer consequences if suppliers are found to be engaged in activities that threaten human health and the environment. The punishment most often comes in the form of negative publicity, lost market share, and the significant energy spent on trying to just get back the reputation lost, let alone rise above it. Significant public outcry and reaction to high-profile issues has given rise to a new field of management—that of corporate supply-chain environmental and social responsibility (SCESR) management.[28] Concerns have also given rise to laws that attempt to prescribe extended producer responsibility (EPR), such as recycling and postconsumer waste-control laws for certain types of items.

In the past two decades, regulations have become common that hold manufacturers responsible for their products at their end of life. Prior to this, it was unprecedented in commercial law that a buyer of an article could turn to the manufacturer of the materials and somehow hold it accountable for the article at its end of life, including packaging materials. Germany's Packaging Ordinance of 1991 assigned producers the financial responsibility for collecting, handling, and recycling/disposing of the packaging waste from products.[29] This was a watershed event in the history of environmental regulations. It brought into scope items in the hands of the ultimate customer, yet assigned financial responsibility for these items to the producer. The hope was that it would encourage the producer to reduce the quantity and improve the attributes of shipment and display packaging sold to the consumer with the product.

More recently, the electronic and electrical equipment (EEE) industries have been rocked by the European Commission Directives 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (the RoHS Directive) and 2002/96/EC on waste electrical and electronic equipment (the WEEE Directive).[30] The directives make producers financially responsible for their products when a consumer needs to dispose of them. The directives also restrict the use of several chemical substances. The laws are forcing the entire global EEE industry to make changes in products and operations. The laws have also not escaped the interest of financial controllers. The Financial Accounting Standards Board (FASB) released FAS 143-1, guidance to address the accounting for obligations associated with the WEEE Directive.

The concept of end-of-life responsibility for waste is alive and well, but also hidden in these directives is yet another even greater challenge—the concepts of sustainable development and the precautionary principle. In 1987, the Brundtland Commission[31] defined sustainable development as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs." The precautionary principle is based on the 1983 World Charter for Nature.[32] The charter states, "Activities which are likely to pose a significant risk to nature shall be preceded by an exhaustive examination; their proponents shall demonstrate that expected benefits outweigh potential damage to nature, and where potential adverse effects are not fully understood, the activities should not proceed."

Together, these principles are now promoted as corporate social responsibility (CSR) and sustainability. The concern here is that a firm should earn its income responsibly with regard to human welfare and the environment, and in doing so not take away from the quality of life for future generations. This focus on the method of making money is different from concerns about what the firm does with its income. Many firms fail to see the difference and then wonder why they are criticized despite generous conservation and philanthropy programs. Meeting the challenges of CSR is daunting for any large manufacturer selling durable goods, and can be ruinous for small and midsize enterprises (SMEs) that get caught up in allegations of unethical CSR behavior.

Ran Goel[33] summarizes 16 international principles used to support CSR and sustainability of the commercial enterprise. The tools profiled in his guidebook include:

1. AccountAbility 1000 Assurance Standard (AA1000)
2. Ceres Principles
3. Equator Principles
4. Extractive Industries Transparency Initiative (EITI)
5. Global Reporting Initiative (GRI) Sustainability Reporting Guidelines
6. Global Sullivan Principles

7. Greenhouse Gas (GHG) Protocol
8. International Labor Organization (ILO) Declaration on Fundamental Principles and Rights at Work
9. ISO 14000
10. MacBride Principles
11. Organization for Economic Cooperation and Development (OECD) Guidelines for Multinational Enterprises
12. Social Accountability 8000 (SA8000)
13. United Nations Global Compact (GC)
14. United Nations Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights
15. Universal Declaration of Human Rights (UDHR)
16. Voluntary Principles on Security and Human Rights

Given the key issue of scope, a wise approach to deciding what aspects and what items to focus on is to start with customer expectations. What are the ecosphere protection factors that are important to the customer? This can vary tremendously across the types of items and the customers for them, but families of items and relationships may have common threads. Customers may already have identified CSR aspects that are important to them, either because of their personal needs, the imposition of an external standard of regulation such as ISO 14001,[34] societal expectations that translate into general market expectations, or all three drivers. As an example, a white goods manufacturing industry might have identified wastewater reduction, material use reduction, air emissions, and energy use conservation as aspects of significance. Labor treatment may be a preeminent concern of the customers of agricultural enterprises.

Smaller suppliers are likely to have difficulty funding and managing the internal labor and/or outside consultants required to analyze, prioritize, and significantly improve the environmental aspects of their operations beyond the obvious and easy-to-attain attributes and practices. In some jurisdictions, local laws and regulatory agency permits and inspections, such as for chemical and waste storage, are likely to be the only drivers of progress at this level. Some regulations may introduce principles of continual improvement, but in general the legally mandated controls will have a uniform position of minimum requirements across business types and sizes. Requirements beyond compliance come from somewhere else, and it is these that will pose more challenges to the small enterprise, because they are not uniform.

An undesirable aspect of the operations of larger multinational corporations is the imposition of a single requirement applied to all suppliers without due consideration of the supplier's size, the environmental and health risks inherent in the production and exchange of the good or service, and the cultural and political norms of the supplier's location(s). Often, demands are blindly sent out by purchasing agents who are just following what they understand to be a mandate from

the corporate office. When faced with a demand that requires considerable effort, make sure that the requestor really intended the demand to be applied to the type of good or service in question. Instead of catering to individual demands that expend valuable time and resources, the best defense of the small firm faced with an onslaught of CSR requests is being able to offer evidence of an established CSR program of reasonable and supportable scope.

When designing a CSR program, firms will need to decide what to expect of suppliers and which suppliers. What environmental and social responsibility attributes does the firm expect? How much of the supply base must comply? Are the requirements general principles, specific criteria, or both? For example, the firm may ask that its top suppliers by spend all have environmental management systems certified to an environmental standard such as ISO 14001. It may be beneficial to investigate and adopt an industry standard code as opposed to inventing a unique one. Unlike environmental management, however, where a relative few international standards have achieved widespread use across industry types, such as ISO 14001, social responsibility codes are more numerous. A single global CSR standard has yet to achieve widespread acceptance and implementation.

Besides deciding what CSR attributes to require and what suppliers to require them of, there is the issue of enforcing the requirements. If suppliers are not in conformance, should they be given time to correct the issue? What happens if a supplier does not correct the issue? Will management support finding an alternative supplier if the transfer involves significant time and/or substantial money? What if production will be down for some time? Should the firm simply trust when suppliers state that they meet the requirements, or should there be verification? What are the ways in which the firm can positively influence its suppliers' operational actions and drive continual improvement, but without directing the operations and possibly becoming potentially liable for direction?

When implementing a supply-chain CSR program, remember the supply chain is a global audience and the program will have to work for small and large enterprises and across geographic and legal boundaries. The best practice is to prioritize suppliers for attention based on those where the maximum improvement in environmental protection can be attained. Focus especially on improvements in areas of global concern that add value to the end customer, such as energy use and waste reduction.

Regulatory requirements are easier to tender than voluntary measures, because these have a legal source and are less likely to be challenged as "blue-sky" and optional. Requirements that prescribe how the supplier is to conduct its own operations are always a problem. Keep the program ethical. The firm should not ask suppliers for more controls than the firm itself has achieved for its own operations. It is acceptable to have goals that push the supplier to improve, but the same goals should apply to the parent firm as well.

An aspect of social responsibility that is often handled separately from supply-chain CSR programs in medium to large enterprises is supplier diversity.

Supplier diversity is the act of giving business preference to suppliers that are disadvantaged because of some issue of common prejudice, such as the size of the firm, or the gender, disability, and ethnic makeup of the firm's ownership and management. Supplier diversity is most often driven by government procurement operations. Multinational companies that work on government-funded projects will be very familiar with supplier diversity as an issue.

The key to any diversity program is to give preference when all other factors of desired results are equal, or when it is believed that the supplier will be able to deliver the desired results as well as or better than any competitor if properly capitalized and supported. Diversity goals are usually stated as a percent of total spend. The goals for commercial work, where implementation is voluntary, are typically higher than goals where compliance is mandatory, such as for government contracts in the United States. Where the driver is compliance with an external mandate, goals are usually limited to the percent of spend within the category of the good or service of concern and the country of origin of the requirement.

Best-in-class firms establish diversity goals internationally, and based on categories of goods and services purchased. Leading firms take the time to develop the diversity supplier, and diversity suppliers are often driven to provide higher levels of service and value in the interest of potential growth. A consequence of the attention can be growth to the point that the firm no longer qualifies for government-recognized diversity status because its revenue is too large. The reliance of the supplier on the firm's purchases and support must be monitored carefully. The firm may start out as a large percentage of the supplier's business. Over the period of development, the firm's contributions should decline to the point that they do not constitute too large a share of the diversity supplier's business, so that if a transition is necessary it will not be an extraordinary loss of revenue for the supplier.

38.17 RECORD KEEPING

The documents that result from the execution of purchasing, such as agreements, orders, inspections, receipts, and invoices, are all examples of records. The prudent firm will determine what records need to be maintained by law or as a necessity of sound business management, and for how long. The best firms will have a published record-retention schedule, procedural guidance, and designated local coordinator to maintain the schedule, guidance, other required paperwork, and communications. Records regarding matters that are subject to legal action should not be altered or destroyed without advice from an attorney.

38.18 TRAINING

Managers at all levels must ensure adequate resources are in place to carry out their operations, and that their employees have the appropriate education, training, skills and experience to fulfill their assigned work responsibilities. The qualifications and training needs of employees should be assessed by their immediate

manager annually or as needed. The manager should compare a description of the skills and/or requirements for a position and the skills, training, education, and experience of the individual. This assessment is best done in conjunction with an annual performance review, providing a feedback process for the employee.

Notes

1. David N. Burt et al., *World Class Supply Management* (New York: McGraw-Hill Irwin, 2003).
2. The Uniform Commercial Code (UCC) applies to commercial transactions within the United States. The UCC is prepared under the joint sponsorship of the American Law Institute (ALI) and the National Conference of Commissioners on Uniform State Laws (NCCUSL). The UCC is available online at www.law.cornell.edu/ucc/ucc.table.html.
3. Burt, *World Class*.
4. Anthony Tarantino, *The Manager's Guide to Compliance* (Hoboken, NJ: John Wiley & Sons, 2006). (Note: Important exemptions for small companies are described in Chapter 6.)
5. The Financial Accounting Standards Board (FASB) is a private sector organization that has established the standards of financial accounting and reporting recognized as authoritative by the Securities and Exchange Commission (SEC) since 1973.
6. The Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745, July 30, 2002), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, is a U.S. federal law passed in response to a number of major corporate and accounting scandals. The legislation establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms, and established the Public Company Accounting Oversight Board (PCAOB), which is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies.
7. The principal international accounting standards are described in Tarantino, *The Manager's Guide to Compliance*, and important exemptions for small companies are described in Chapter 6 therein.
8. The lists are available online at www.cbp.gov/xp/cgov/export/persons_list/.
9. Tarantino, *Manager's Guide*.
10. For more information, see the Department of Justice web site at www.usdoj.gov/criminal/fraud/fcpa.html.
11. Tarantino, *Manager's Guide*.
12. Tarantino, *Manager's Guide*.
13. Ibid.
14. The Society of Manufacturing Engineers (SME) is a good source of learning materials about these concepts. See www.sme.org/.
15. Tarantino, *Manager's Guide*.
16. The International Business Forum provides information about business opportunities in the international marketplace. It is intended for companies wishing to export or expand into foreign markets as well as for those interested in acquiring products and services from other countries. See www.ibf.com/.

17. The Taxation and Customs Union of the European Commission develops and operates several databases in conjunction with member states' customs and taxation services. These can be found online at http://ec.europa.eu/taxation_customs/common/databases/index_en.htm.
18. The World Trade Organization maintains an online "Valuation Gateway" at www.wto.org/english/tratop_e/cusval_e/cusval_e.htm.
19. Its web site (at www.fta.gov.sg) includes many helpful documents, a tariff savings calculator, and links to other free trade organizations.
20. More information about the CEPA can be found at www.tdctrade.com/cepa/.
21. See www.aseansec.org.
22. Reviews have been completed and published for 22 members and nonmembers. The reviews are available under the topic of "Competition" at www.oecd.org/maintopic/.
23. The European Commission maintains a web site for competition at which the various laws and rules may be found: http://ec.europa.eu/comm/competition/index_en.html.
24. U.S. Code is available online at www.gpoaccess.gov/uscode/index.html.
25. Quality Management, The ISO 9000 Family of International Standards, International Organization for Standardization, www.iso.org/iso/en/prods-services/otherpubs/iso9000/index.html.
26. Tarantino, *Manager's Guide*.
27. Burt, *World Class*.
28. Additional information about these concepts is available through the United Nations Environmental Program, Supply Chain Management Tools (see www.uneptie.org/pc/pc/tools/supplychain.htm).
29. Bette K. Fishbein, "EPR: What Does It Mean? Where Is It Headed?," *Pollution Prevention Review* 8 (1998): 2.
30. Information about the directives is available online at the European Commission environment web site at http://ec.europa.eu/environment/waste/weee_index.htm.
31. Report of the World Commission on Environment and Development, "Our Common Future," Official records of the United Nations General Assembly, 42nd Session, Item 83 of the provisional agenda, A/43/427, August 4, 1987.
32. Official records of the United Nations General Assembly, 48th Plenary Meeting, Item 37/7, A/RES/37/7, October 28, 1983.
33. Ran Goel, "Guide to Instruments of Corporate Responsibility," Pensions at Work, Social Investment of Pension Funds, University-Union Research Alliance, October 2005.
34. Environmental Management, The ISO 14000 Family of International Standards, International Organization for Standardization, www.iso.org/iso/en/prods-services/otherpubs/iso14000/index.html.

CHAPTER 39

TELECOMMUNICATIONS

Angelia Fitts

Note: The views expressed in this chapter are those of the author and are not necessarily those of AT&T or any of its subsidiaries.

The telecommunications industry has experienced unprecedented change over the past three decades. Fueled by a global economy and the advent of new technologies, few industries have experienced the sustained growth, success, and competition that telecom companies have. This success has a cost, though, and telecom companies have faced often confusing and ever-increasing regulation and compliance requirements. As new products and services converge and cross over traditional boundaries, compliance regulations will need to be reassessed and adjusted to protect consumers and promote competition.

In this chapter, we review general regulations and compliance requirements facing telecom companies. Although specific regulations vary by country and locality, requirements are similar in regard to environmental health and safety, antitrust, privacy and security of customer information, and regulated pricing and tariffs. We discuss recent and emerging issues, such as privacy and adult content, that impact the fastest growing segments of the telecom industry.

39.1 LICENSES

The Communications Act of 1934 established the Federal Communications Commission (FCC) in the United States to regulate interstate and international communications by radio, television, wire, satellite, and cable. Frequencies are assigned

and licensed by the FCC, and there are strict penalties for transmission of signals outside of the defined use or without an approved license.

Spectrum assignment and management are normally contentious issues because of the limited spectrum available and the multiple competitors seeking more bandwidth for the multiple services and products offered.

The FCC also sets standards for service quality and rural availability for certain services. The Telecommunications Act of 1996,[1] under the universal service provisions, guarantees the availability of quality phone services to households at affordable rates. It also asserts that all areas of the country should have access to advanced telecommunication and information services (such as high-speed Internet), and that rural and high-cost areas receive services at prices comparable to urban areas.

39.2 REGULATED PRICING AND TARIFFS

Pricing regulations vary in the telecom industry based on the competitive maturity of the marketplace. Monopoly markets, such as state-owned wireline communications and cable companies, tend to require pricing according to the customers' *ability* to pay. Pricing for highly competitive markets is driven by what the customers are *willing* to pay given the other available offerings. Once a service is recognized as competitive, tariffs generally are no longer applicable, although some tariffs remain in effect.

Regulators, in their attempt to promote competition and provide services to a wide range of constituents, permit service providers to impose additional charges to cover the cost of providing services. Common subsidies include network infrastructure or maintenance charges, emergency services fees, connection fees, and other subsidies to cover the cost of providing service to rural geographical areas. In the United States, the FCC directs the Universal Service Fund (USF). The USF supports telecommunications services in high-cost areas and for low-income subscribers, rural health-care providers, and schools and libraries. The federal USF charge, adjusted quarterly, is assessed as a percentage on all interstate services, international long distance, private lines, and end-user access charges. Although the federal USF subsidy still exists, the majority of U.S. subsidies have disappeared, allowing U.S. companies to compete in the global marketplace.

Regulated pricing is generally arrived at through complex calculations based on predefined criteria and submitted to regulatory agencies annually for approval. Prices are determined separately for recurring fees (e.g., monthly service fees); nonrecurring fees (e.g., reconnection or cancellation fees); and usage-based charges.

As competition and service availability increase, pricing regulations generally decrease. The telecom industry is rapidly moving from deregulation to fierce competition, and those companies traditionally in the highly regulated space, such as wireline companies, are aggressively seeking relief from regulatory pricing in

order to offer a wide range of unbundled services at competitive prices. Regulatory relief is emerging in Europe as well, as telecom companies seek the repeal of regulatory taxes in order to allow traditional wireline companies to compete with cable providers. As the telecom market gains competitiveness, tariff and regulatory pricing will diminish and most likely be limited to emergency and other social services.

39.3 HEALTH AND SAFETY

General health and safety regulations generally fall into either environmental or public safety. Compliance requirements related to environmental health and safety compel communication networks to have satisfactory levels of safety during construction, operation, and maintenance. Public safety standards include emergency services and aviation.

(a) ELECTRONIC SAFETY. Equipment should be protected against the harmful effects of insulation failure, defects between circuits with different voltages, and other unwanted high voltages caused by electrical production plants, electric power, or lightning discharges. Technicians and other workers need to take precautions against electrocution or damage to other utility equipment during installation due to the close proximity of communication equipment to power sources, water lines, gas lines, and other utilities.

(b) HAZARDOUS MATERIALS AND WASTE. In the United States, the Clean Water Act, Clean Air Act, Pollution Prevention Act, and the Resource Conservation and Recover Act establish the basic requirements, enforced by the Environmental Protection Agency (EPA), for the management and discharge of pollutants and hazardous materials. Examples of telecommunication business activities subject to these regulations include vehicle emissions, backup generators and power supply, legal disposal of batteries, and the storage of hazardous materials such as sulfuric acid, lead, diesel fuel, and propane. Companies are required to report hazardous materials quantities at cell sites, switches, warehouses, and administrative offices.

(c) PUBLIC SAFETY. General public safety regulations include the clear marking of above- and below-ground cables and accurate record keeping for facilities. Companies with above-ground facilities must also ensure that tall antennae, approximately 200 feet or more, are clearly marked with flashing lights for lowflying aircraft.

Single emergency call numbers, such as 112 in the European Union and 911 in the United States, provide emergency response via location-based services using the caller's number to locate the origination point. The wide availability of wireless technologies has given rise to enhanced location-based services, known as E-911 and E-112. In Europe, legislators are considering equipping all automobiles with automated emergency call technology (eCall) by 2009.

Enhanced location-based services are expensive to implement, and virtually all countries are allowing providers to pass on some charges to subscribers to cover implementation and coverage to rural areas.

39.4 PRIVACY AND SECURITY OF CUSTOMER INFORMATION

In the United States, the Telecommunications Act of 1934[2] established the basic requirements that all telecommunication providers have the duty to protect the confidentially of customer proprietary information, including the quantity, type, destination, and amount of use of telecommunication services. Thus, telecom providers are prohibited from sharing information with external parties unless the request meets specific guidelines, like those under legal subpoenas or emergency calls placed by the user.

Pretexting and social engineering—using false and/or illegal pretenses to obtain confidential information from service providers—is becoming much more widespread. In response, many regulatory agencies require, or are considering requiring, mandatory customer passwords, encryption, and public notice of security breaches.

The EU privacy directives[3] go further in legislating customer privacy than U.S. regulations and are a good indication of the future of privacy laws in other countries. The EU directives, established in 2002, provide for the protection of privacy in the electronic communications sector and the processing of personal data. Specifically, the directives prohibit unsolicited marketing and the use of data related to customer usage (also known as traffic data) unless customers give permission (opt in). However, customers must opt out if they don't wish to be included in public directories.

The collection and use of location data—data regarding the physical location of a user over a specified period of time—is the subject of much debate and attention in the legislative and political arenas. The EU privacy directives require that providers obtain explicit permission from the customer in order to collect or use location data. Questions that need to be addressed include how long service providers should be allowed or required to retain data regarding a customer's usage, such as e-mails sent, Internet sites visited, and detailed phone records.

An example may illustrate the difficulty in determining how to proceed in answering these questions. Assume that a family of three, including a teenager, subscribes to cellular services. The cellular company has a new location-based service using Global Position System (GPS) that will allow the parents to search for nearby restaurants or the teenager to locate friends who also have subscribed to the service. This same technology can be used by the parents as a virtual nanny to receive alerts if the teenager goes beyond a specific physical boundary or to trace the specific location of the teenager's phone in case of emergency.

Information gathered in providing these services can also be used for other purposes perhaps unknown to the family. Marketers can use the data to research

traffic and usage patterns for consumers for general or specific marketing purposes. Content providers could sell services to provide unwelcome content or unsolicited marketing. The same technology and data gathered could be used by law enforcement as a virtual tracking device for suspects or as evidence in a legal proceeding. A predator could also obtain the whereabouts of an unsuspecting victim.

The potential uses of these services are virtually limitless, as are the unanswered questions. What level of approval is the service provider required to obtain from the family to protect each individual's rights? Is the explicit approval of the responsible (paying) party enough, or does the teenager have the right to privacy and need to grant permission for her parents to use the nanny service? How will this permission be tracked, obtained, and secured to protect the family? What data retention or deletion requirements are necessary to meet the needs of service providers, law enforcement, or other interests? Can the data be used for marketing purposes, and, if so, will the consumer be protected from unwelcome spamming or age-inappropriate content? What security needs to be in place to prevent unauthorized individuals from using the service or obtaining location data?

Specific guidance is generally unavailable or unclear, and will likely be regulated in the near future and framed by each country's constitutional freedoms and customs.

39.5 CONTENT

Content-based telecommunication services have been receiving significant attention in the past decade and will continue to be a topic of much debate.

One viewpoint is that telecommunication providers are responsible for the content of all communications transmitted and liable for inappropriate use. At the other end of the spectrum is the viewpoint that communications should be completely free, open, and dictated by the users, not regulators or telecommunication companies. The majority of proposed legislation falls between these two extremes.

Telecommunication companies have self-regulated in the past to forestall governmental regulation. The Telecommunication Act of 1996 threatened to establish a rating system for video programming if not enacted voluntarily by the industry. The U.S. broadcasting industry responded by establishing a parental rating system voluntarily broadcasted. In 1998, the FCC adopted technical requirements for consumer electronic equipment to enable blocking of television programming based on these ratings (commonly referred to as the "V-chip"). Many countries have similar rating systems, and some, like the Netherlands, have begun extending the use of their ratings to other communication media, including gaming and the Internet.

Drawing on the success of self-regulations in the entertainment and cable industries, some telecoms, especially wireless, are researching V-chip-type

parental control technology. Internet providers have relied on consumers to protect themselves with available software to block unwanted content. Current decency laws vary by country and guide the requirements regarding the blocking of adult content such as pornography and gambling to underage subscribers.

Receiving unsolicited content on wireless phones is an especially hot topic in countries where subscribers are charged for incoming calls. In Europe, where the calling party pays for wireless calls, unsolicited calls are merely an annoying nuisance. However, subscribers in areas where they are billed for all usage generally frown upon getting billed for sales calls to join a local gym or text messages to enhance your libido.

As the convergence and sophistication of technologies continue to develop, the telecommunications industry will need to respond to the regulatory changes and legal questions generated around security, privacy, availability, and limited spectrum. Company compliance directors and other interested individuals should definitely stay tuned for updates in the legislative area.

Notes

1. Telecommunication Act of 1996, Pub. L. No. 104–104, 110 Stat. 56 (47 U.S.C.).
2. U.S. Communications Act of 1934, Ch. 652, 48 Stat. 1064 (amended 1996).
3. EU Directive 2002/58/ECEC, published in the Official Journal at OJ L 201/37 on July 31, 2002.

CHAPTER 40

CARRIERS COMPLIANCE IN FREIGHT TRANSPORTATION AND LOGISTICS

David Jacoby

40.1 INTRODUCTION

Rules and regulations in the transportation and logistics field may be grouped into two categories: (1) regulation that affects carriers (transportation and logistics companies providing freight movement services) and (2) regulation that affects shippers (companies that hire others to move freight). The government imposes many regulations on carriers that shippers may not be aware of. Conversely, many shippers are unaware of the regulations imposed on the carriers that they hire.

Accordingly, this chapter highlights significant regulations faced by carriers, and a separate one (Chapter 34) focuses on regulations affecting

shippers—companies hiring other companies to move freight. Both provide an overview of the bodies of law affecting each group so both shippers and carriers may have an appreciation for the regulatory environment affecting each other, as well as a familiarity with the most common laws that could affect their businesses.

Carriers need to understand and comply with a range of laws that have developed over many years and are in some cases quite complex. The requirements vary substantially by mode. Therefore, the chapter is structured by type of transport: truck, rail, water, and air.

This chapter focuses on freight, not passenger, transport, and uses the United States as a reference point for defining compliance issues. Because of the legislative nature of compliance issues, the institutional and regulatory framework is different outside of the United States.

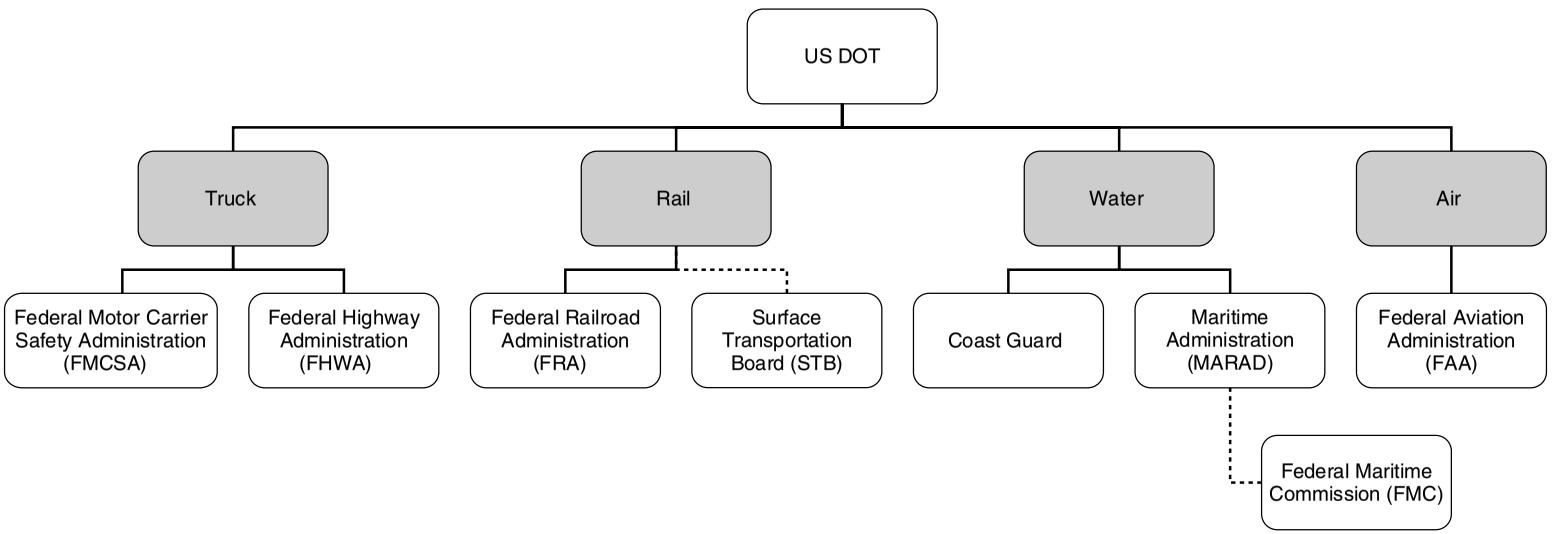
40.2 KEY REGULATORY BODIES

In the United States, the Department of Transportation (DOT) exercises authority over freight carriers through the following agencies,[1] which are shown in Exhibit 40.1.

- *Trucking companies.* The Federal Motor Carrier Safety Administration (FMCSA) sets truck size and weight limits and Hours of Service rules, among others. Also, the Federal Highway Administration (FHWA) certifies the safety of new trucking companies.
- *Railroads.* The Federal Railroad Administration (FRA) administers rail safety and rail assistance programs and research efforts. Also, the Surface Transportation Board (STB) resolves railroad rate and service disputes and reviews proposed railroad mergers. The STB is organizationally independent of the DOT, as indicated by the dashed line in Exhibit 40.1.
- *Marine transportation providers.* The Maritime Administration (MARAD) administers the cargo preference rules, and the Federal Maritime Commission (FMC) administers laws designed to protect U.S. interests in the ownership of waterborne carriage and terminal operation. The Coast Guard serves ports and inland waterways, and has the right to inspect cargoes.
- *Air cargo carriers.* The Federal Aviation Administration (FAA) oversees the air traffic control system, intervenes to prevent aviation-related environmental side effects, and mandates airworthiness certification of new aircraft.

40.3 COMPLIANCE ISSUES FOR TRUCKING COMPANIES

The Motor Carrier Act of 1980 deregulated the trucking industry. In 1995, the Interstate Commerce Commission (ICC) was terminated and some of its responsibilities transferred to the Surface Transportation Board (STB). This move effectively institutionalized the 25-year trend toward deregulation. That being said, several important regulations affect trucking companies today.



Source: Boston Logistics Group.

EXHIBIT 40.1 U.S. GOVERNMENT AGENCIES AFFECTING CARGO CARRIER COMPLIANCE

(a) HOURS OF SERVICE. Hours of service (HOS) regulation took effect in 2004. The regulation limits the number of hours that drivers can work in one stretch. Truckers may not drive after being on duty for 60 consecutive hours in a seven-day period or 70 hours in an eight-day period. A "weekend" off (34 consecutive hours) is required to restart the on-duty cycle. Long-haul drivers can drive for 11 hours after 10 consecutive hours off-duty. Drivers using the sleeper berth provision must take at least eight consecutive hours in the sleeper berth, plus two consecutive hours either in the sleeper berth, off duty, or any combination of the two, and may not drive beyond the 14th hour after coming on duty, following 10 consecutive hours off duty.

(b) VEHICLE SIZE AND WEIGHT LIMITS. Allowable truck size and weight limits are defined by 23 CFR (Code of Federal Regulations) Part 658. Size and weight restrictions vary by state and city. In addition, federal and state governments have defined numerous provisions for special vehicles. The itemization of prohibited conditions is lengthy, but the following list of generally allowable conditions may be helpful:[2]

- *Length.* Trailers between 28 and 48 feet long and buses up to 45 feet long are allowed. In addition, nonconforming vehicles that were in lawful operation before 1982 are allowed if they have filed for exemption.
- *Width.* Vehicles under 102 inches wide are generally allowed (Hawaii allows 108-inch-wide vehicles). With state permits, manufactured houses that exceed 102 inches and vehicles with safety and/or non-cargo-carrying appurtenances extending beyond 3 inches from the side of the vehicle are allowed.
- *Weight.* Vehicles are limited to:
  - Gross vehicle weight less than 80,000 pounds (except where lower gross vehicle weight is dictated by the bridge formula[3])
  - Per single axle: 20,000 pounds
  - Per tandem axle combination: 34,000 pounds
  - Tire loads of less than 500 pounds per inch of tire or tread width on nonsteering axles

(c) ADVANCE MANIFEST NOTIFICATION FOR IMPORTS. Trucks entering the United States from Canada or Mexico must have U.S. Customs data processed a minimum of one hour before the shipment arrives at the border, as stipulated by Customs and Border Protection (CBP) in its Final Rule on the Trade Act of 2002.[4]

(d) CREDENTIALING OF HAZARDOUS MATERIALS DRIVERS. Section 1012 of the Patriot Act[5] requires drivers of vehicles transporting hazardous materials to gain state approval that the individual does not constitute a security threat.

(e) SAFETY REVIEW FOR NEW CARRIERS. According to Title 49, "The Secretary shall require, by regulation, each owner and each operator granted new operating authority, after the date on which section 31148(b) is first implemented,

to undergo a safety review within the first 18 months after the owner or operator, as the case may be, begins operations under such authority."

(f) OTHER FMCSA REGULATIONS. In addition the aforementioned regulations, the Federal Motor Carrier Safety Administration (FMCSA) maintains enforcement power over a variety of other laws, embodied in 23 CFR and shown in Exhibit 40.2.

40.4 COMPLIANCE ISSUES FOR RAILROADS

The most significant government act affecting the rail industry in the past 50 years was the Staggers Act of 1980. The combination of the Staggers Act, which ended the regulation of common carrier tariffs, and the Motor Carrier Act, which deregulated trucking, resulted in a shift of traffic from railroads to trucking companies. Though there have been some moves to reregulate the rail industry,[6] often driven by captive shipper situations, carrier compliance issues are much reduced compared to previous years. The rest of this section summarizes some of the more notable compliance issues for rail carriers today.

(a) SECURITY COMPLIANCE. Section 102 of the Rail Safety Reauthorization Bill S. 1402 (2003) requires railroads to comply with DOT security programs.

(b) RAIL SAFETY AND ACCIDENT REPORTING. Section 101 of the Rail Safety Reauthorization Bill S. 1402 (2003) requires railroads and states to provide DOT with safety statistics.

The Rail Safety Reauthorization Bill S. 1402 (2003) also includes a provision that requires "the Federal Railroad Administration's (FRA) Railroad Safety Advisory Committee to develop, and report to Congress, consensus recommendations on changes needed to address fatigue management for covered service employees." These changes would apply to the railroads once finalized.

Also, 49 CFR Part 225 requires carriers to notify the FRA of accidents and incidents, file a monthly accident report, and have an internal control plan containing 11 specified components that describes how the railroad achieves compliance with the regulation (§ 225.33).

(c) NOISE LIMITS. Section 103 of the Rail Safety Reauthorization Bill sets rail noise limits.

(d) FREIGHT TRAINS OPERATING ON PASSENGER LINES. The FRA imposes safety regulations related to freight trains running on passenger lines, and vice versa. For example, high-speed passenger trains operating on a freight line must be able to withstand one million pounds of force without deformation.

(e) OTHER TITLE 49 REGULATIONS. Title 49 includes a variety of other provisions related to railroad safety that would be relevant to those needing comprehensive information on this topic. Its contents include the numbered sections listed in Exhibit 40.3 and Exhibit 40.4.

Part 40 – Drug and alcohol regulations
Part 325 – Compliance with interstate motor carrier noise emission standards
Part 350 – Commercial motor carrier safety assistance program
Part 355 – Compatibility of state laws and regulations affecting interstate motor carrier operations
Part 356 – Interpretations and routing regulations
Part 360 – Fees for motor carrier registration and insurance
Part 365 – Rules governing applications for operating authority
Part 366 – Designation of process agents by motor carriers and brokers
Part 367 – Standards for registration with states
Part 368 – Application for certificates of registration by foreign motor carriers and foreign motor private carriers
Part 370 – Principles and practices for the investigation and voluntary disposition of loss and damage claims and processing salvage
Part 371 – Brokers of property
Part 372 – Exemptions, commercial zones, and terminal areas
Part 373 – Receipts and bills
Part 374 – Passenger carrier regulations
Part 375 – Transportation of household goods in interstate commerce; consumer protection regulations
Part 376 – Lease and interchange of vehicles
Part 377 – Payment of transportation charges
Part 378 – Procedures governing the processing, investigation, and disposition of overcharge, duplicate payment, of overcollection claims
Part 379 – Preservation of records
Part 380 – Special training requirements
Part 381 – Waivers, exemptions, and pilot programs
Part 382 – Controlled substances and alcohol use and testing
Part 383 – Commercial driver's license standards and requirements
Part 384 – State compliance with commercial driver's license program
Part 385 – Safety fitness procedures
Part 386 – Rules of practice for motor carrier, broker, freight forwarder, and hazardous materials proceedings
Part 387 – Minimum levels of financial responsibility for motor carriers
Part 388 – Cooperative agreements with states
Part 389 – Rulemaking procedures—federal motor carrier safety regulations
Part 390 – General
Part 391 – Qualifications of drivers and longer combination vehicle (LCV) driver instructors
Part 392 – Driving of motor vehicles
Part 393 – Parts and accessories necessary for safe operation
Part 395 – Hours of service of drivers
Part 396 – Inspection, repair, and maintenance
Part 397 – Transportation of hazardous materials; driving and parking rules
Part 398 – Transportation of migrant workers
Part 399 – Employee safety and health standards
Part 571 – Federal motor vehicle safety standards

Source: Federal Motor Carrier Safety Administration (FMCSA).

EXHIBIT 40.2 23 CFR REGULATIONS AFFECTING MOTOR CARRIERS

200 Informal rules of practice for passenger service
201 Formal rules of practice for passenger service
207 Railroad police officers
209 Railroad safety enforcement procedures
210 Railroad noise emission compliance regulations
211 Rules of practice
212 State safety participation regulations
213 Track safety standards
214 Railroad workplace safety
215 Railroad freight car safety standards
216 Special notice and emergency order procedures: railroad track, locomotive, and equipment
217 Railroad operating rules
218 Railroad operating practices
219 Control of alcohol and drug use
220 Railroad communications
221 Rear-end marking device—passenger, commuter, and freight trains
222 Use of locomotive horns at public highway-rail grade crossings
223 Safety glazing standards—locomotives, passenger cars, and cabooses
225 Railroad accidents/incidents: reports classification and investigations
228 Hours of service of railroad employees
229 Railroad locomotive safety standards
230 Steam locomotive inspection and maintenance standards
231 Railroad safety appliance standards
232 Brake system safety standards for freight and other nonpassenger trains and equipment; end-of-train devices
233 Signal systems reporting requirements
234 Grade crossing signal system safety
235 Instructions governing applications for approval of a discontinuance or material modification of a signal system or relief from the requirements of Part 236
236 Rules, standards, and instructions governing the installation, inspection, maintenance, and repair of signal and train control systems, devices, and appliances
238 Passenger equipment safety standards
239 Passenger train emergency preparedness
240 Qualification and certification of locomotive engineers
241 U.S. locational requirement for dispatching of U.S. rail operations
244 Regulations on safety integration plans governing railroad consolidations, mergers, and acquisitions of control
245 Railroad user fees
250 Guarantee of certificates of trustees of railroads in reorganization
256 Financial assistance for railroad passenger terminals
260 Regulations governing loans and loan guarantees under the railroad rehabilitation and improvement financing program
261 Credit assistance for surface transportation projects
265 Nondiscrimination in federally assisted railroad programs
266 Assistance to states for local rail service under Section 5 of the Department of Transportation Act
268 Magnetic levitation transportation technology deployment program

Source: Code of Federal Regulations, National Archives and Records Administration.

EXHIBIT 40.3 TITLE 49 REGULATIONS AFFECTING RAILROADS, ADMINISTERED BY THE FRA

1001 Inspection of records
1002 Fees
1003 Forms
1004 Interpretations and routing regulations
1005 Principles and practices for the investigation and voluntary disposition of loss and damage claims
1007 Records containing information about individuals
1011 Board organization; delegations of authority
1013 Guidelines for the proper use of voting trusts
1014 Enforcement of nondiscrimination on the basis of handicap in programs or activities conducted by the STB
1016 Special procedures governing the recovery of expenses by parties to Board adjudicatory proceedings
1018 Debt collection
1019 Regulations governing conduct of Board employees
1021 Administrative collection of enforcement claims
1033 Car service
1034 Routing of traffic
1035 Bills of lading
1037 Bulk grain and grain products—loss and damage claims
1090 Practices of carriers involved in the intermodal movement of containerized freight
1104 Filing with the Board-copies-verification-service-pleadings, generally
1105 Procedures for implementation of environmental laws
1106 Procedures for safety integration plans involving railroad consolidations, mergers, and acquisitions of control
1120 Use of 1977–1978 study of motor carrier platform handing factors
1132 Protests requesting suspension and investigation of collective rate-making actions
1133 Recovery of damages
1135 Railroad cost-recovery procedures
1139 Procedures in motor carrier revenue proceedings
1141 Procedures to calculate interest rates
1144 Intramodal rail competition
1146 Expedited relief for service emergencies
1147 Temporary relief under 49 U.S.C. 10705 and 11102 for service inadequacies
1150 Certificate to construct, acquire, or operate railroad lines
1151 Feeder railroad development program
1152 Abandonment and discontinuance of rail lines and rail transportation under 49 U.S.C. 10903
1180 Railroad acquisition, control, merger, consolidation project, trackage rights, and lease procedures
1182 Purchase, merger, and control of motor passenger carriers
1184 Motor carrier pooling operations
1242 Separation of common operating expenses between freight service and passenger service for railroads
1243 Quarterly operating reports—railroads
1244 Waybill analysis of transportation of property—railroads
1245 Classification of railroad employees; reports of service and compensation
1247 Report of cards loaded and cars terminated
1248 Freight commodity statistics
1253 Rate-making organization; records and reports
1280 Handling of national security information and classified material
1300 Disclosure, publication, and notice of change of rates and other service terms for rail common carriage
1305 Disclosure and notice of change of rates and other service terms for pipeline common carriage
1310 Tariff requirements for household goods carriers
1313 Railroad contracts for the transportation of agricultural products
1332 Filing contracts for surface mail transportation

Source: Code of Federal Regulations, National Archives and Records Administration.

EXHIBIT 40.4 TITLE 49 REGULATIONS AFFECTING RAILROADS, ADMINISTERED BY THE STB

40.5 COMPLIANCE ISSUES FOR MARINE TRANSPORTATION COMPANIES

The level of regulation in today's marine shipping industry is light compared to historical levels.

Since 1928, the U.S. government has offered subsidies and incentives to try to assure stability and continuity for the maritime industry, and to ensure that the merchant fleet could be deployed to support wartime operations if necessary.

- The Merchant Marine Act of 1928 encouraged U.S. shipbuilding, and the 1936 Merchant Marine Act established the Merchant Marine Academy. The Merchant Marine Act of 1970, signed by President Ronald Reagan, called for the construction of 300 merchant ships and provided for substantial tax breaks for those companies investing in new shipping, presumably suggested by the bill and subsidized by the 1936 moratorium on new shipping program applications in 1981.
- Construction differential subsidies motivated U.S.-flag carriers to invest in shipbuilding, while operating differential subsidies offset the subsidies received by many foreign-flag carriers.

Despite the incentives, however, the U.S. ocean shipping industry became uncompetitive[7] and the industry was eventually largely deregulated.[8] As the true cost of U.S. shipbuilding and crewing became apparent, many shipping companies were sold to foreign entities[9] or migrated to tax havens such as Panama, Liberia, Costa Rica, Hong Kong, and Gibraltar. Panama has no income tax on earnings outside of Panama, no share issuance time limits, and no annual filing requirements for tax returns or financial statements.

Today, compliance in the ocean shipping industry centers around cabotage, cargo preference, and the 24-hour manifest rule.

(a) CABOTAGE. The Jones Act of 1920, also called the Merchant Marine Act, restricted coastwise trade to U.S.-flag vessels and mandated that American-flag vessels be constructed in the United States and owned by U.S. nationals. The Jones Act is still in effect today.

(b) CARGO PREFERENCE. Since 1904, government legislation has favored U.S.-flag vessels for shipment of government-impelled cargo. The following text, adapted from the Maritime Administration (MARAD), outlines the cargo preference laws:

- "The Cargo Preference Act of 1904 (1904 Act) requires all items procured for or owned by U.S. military departments and defense agencies be carried exclusively (100 percent) on U.S.-flag vessels available at rates that are not excessive or otherwise unreasonable. These cargoes are generated primarily by Department of Defense (DOD) contracts with domestic and foreign

contractors. Cargo preference applies not only to the end product but also to component parts.

- "The Cargo Preference Act of 1954 (P.L. 83-664), as amended, requires that at least 50 percent of the gross tonnage of all Government-generated cargo be transported on privately owned, U.S.-flag commercial vessels to the extent such vessels are available at fair and reasonable rates. In 1985, the Merchant Marine Act of 1936 was amended to require that the percentage of certain agricultural cargoes to be carried on U.S.-flag vessels be increased from 50 to 75 percent.
- "Section 901(a). Section 46 U.S.C. 1241(a) requires any officer or employee of the United States traveling on official business overseas or to or from any of the possessions of the United States, unless otherwise noted, must travel and transport his personal effects on ships registered under the laws of the United States.
- "The Food Security Act of 1985 amended the Cargo Preference Act of 1954 in order to increase the minimum U.S.-flag requirement from 50 to 75 percent for shipments of agricultural cargoes under certain foreign assistance programs of the United States Department of Agriculture and the Agency for International Development.
- "P.L. 105-383 established that substandard vessels and vessels operated by operators of substandard vessels are prohibited from the carriage of Government-impelled cargo for up to one year after such determination has been electronically published.
- "Public Resolution (PR) 17 (48 Stat. 500) of the 73rd Congress requires that all cargoes generated by an instrumentality of the Government, such as the Export-Import Bank of the United States, be shipped (100 percent) on U.S.-flag vessels, unless a waiver is granted by the Maritime Administration.
- "The Maritime Security Act of 1996, Section 17 of the 1996 Act, permits Great Lakes ports to participate in the handling of P.L. 480 Title II humanitarian food aid packaged commodities awarded on a lowest landed cost basis without reference to vessel flag. The law allows these ports to act as bridge-ports, providing loading and unloading services, even though the cargo actually may be shipped from another port, and thus provides stevedoring jobs during the winter months when the Great Lakes are closed to vessel traffic."

Another form of cargo preference occurs in the fishing industry. Vessel operators associated with fisheries must be at least at least 75 percent owned by American nationals and be under American control, including directorship, voting rights, and other criteria. According to the American Fisheries Act of 2002, "the owners and operators of all the member vessels that are signatories to a fishery cooperative are . . . responsible for compliance with the requirements of this section."

(c) CARGO SECURITY AND INSPECTION RULES. The 24-hour rule, instituted in 2002 and still in effect today, mandates that shipping companies must submit a manifest to U.S. Customs at least 24 hours prior to loading for any goods on a ship to call at or leave a U.S. port.

Also instituted as a security measure, Title 49 Sections 450–453 give the Coast Guard the right to inspect cargo containers used in international transport.

(d) OTHER REGULATIONS AFFECTING MARINE CARGO. The Transportation Security Administration (TSA) and the Coast Guard are working toward effective hiring and human resources practices and standard Transportation Worker Identification Credentials (TWIC). The idea is to pilot one standard identification card that can be used across all modes of transportation, but the program is still under development, and there are currently no compliance requirements related to it.

For additional information on regulations affecting ocean cargo, refer to MARAD or the FMC.

40.6 COMPLIANCE ISSUES FOR AIR CARGO CARRIERS

The airline industry is largely deregulated today. The Civil Aeronautics Board, founded in 1938, regulated routes, prices, and most aspects of airline operations. The Federal Aviation Administration (FAA), which was formed in 1967 to deal with the increasing requirements of air traffic control, took over its responsibilities. The Airline Deregulation Act of 1978 had the effect of focusing the FAA's responsibilities on safety.

Since the terrorist events of September 11, 2001, the major focus of both cargo and passenger airline compliance has been related to security. The TSA creates and directs security programs through the sky marshal and other air security programs.

(a) MANDATED SECURITY MEASURES. The Aviation and Transportation Security Act (ATSA) of 2001, passed shortly after the terrorist attacks of 9/11/2001, empowers the TSA to:

- Take over civil aviation security functions.
- Require screening of airport security personnel.
- Require improved flight deck integrity and protection measures.
- Authorize sky marshals to carry firearms and arrest suspects without a warrant. Airlines must provide seats to sky marshals at no cost.
- Mandate pilot programs to test new security technologies in 20 airports.
- Mandate cooperation in cabin crew training for security conditions. "Each air carrier shall develop a flight and cabin crew training program in accordance with that guidance and submit it to the Administrator for approval."
- Mandate pass-through of the security costs associated with these: "The Under Secretary of Transportation for Security shall impose a uniform fee, on passengers of air carriers and foreign air carriers in air transportation

and intrastate air transportation originating at airports in the United States, to pay for the ... costs of providing civil aviation security services."

In a related set of rules, Title 49 requires carriers to share the burden of developing and implementing these safety programs:

- Parts 1544 and 1546 require domestic and foreign carriers, respectively, to carry out security programs that comply with this regulation.
- Part 1548 requires indirect carriers such as freight forwarders to participate and cooperate with the programs that their partners are mandated to execute.
- Part 1552 prohibits flight schools from providing flight training to aliens without gathering certain security-related information and providing it to the TSA.
- Part 1562 restricts access to airports in and close to Washington, D.C.[10]

Also, in FAA-2003-14825-64, the FAA requires certification of airworthiness for new aircraft.

(b) LIMITS ON FOREIGN OWNERSHIP. The Air Commerce Act of 1926 bars foreign carriers from owning more than 49 percent of domestic airlines shares and the Civil Aeronautics Act of 1938 bars them from controlling more than 25 percent of their voting rights. The case for regulation of foreign ownership of airlines has been questioned in recent times. The airline industry may have enough carriers to assure adequate service; but many countries regulate foreign ownership as a matter of national security, public safety, and economic security.

(c) MAINTENANCE RECORDS MANAGEMENT. Airlines must maintain highly disciplined maintenance records as a matter of public safety. Regulation 14 CFR (Code of Federal Regulations) Part 91.417 (for maintenance) and 14 CFR Part 43.9 (for repairs), specifies the detail to which work orders must be recorded and maintained. The regulation requires "records of the maintenance, preventive maintenance, and alteration and records of the 100-hour, annual, progressive, and other required or approved inspections, as appropriate, for each aircraft (including the airframe) and each engine, propeller, rotor, and appliance of an aircraft." The records must include a detailed description of work performed, dates, and signatures of the mechanics or maintenance management certifying airworthiness.

Although the records can be discarded once the work is completed again or after 12 months, they are almost always retained because complete records are vital to resale value.

(d) OTHER REGULATIONS AFFECTING AIR CARGO. For additional information on regulations affecting ocean cargo, the reader is referred to the TSA and the FAA.

40.7 CONCLUSION

The transportation industry has been substantially deregulated in recent years. However, the rise of terrorism has led to a heightened need for consistent security protocols. The need for increased security, combined with a renewed emphasis on safety, has transformed the regulatory environment from one focused largely on protectionism to one focused on safe and secure global transportation—a goal that, while less contentious, will undoubtedly be a continual challenge to achieve.

Notes

1. Several agencies within DOT administer compliance of state DOTs to federal standards; however, these agencies place few or no regulations on freight carriers or shippers. These agencies include:
   - The National Highway Traffic Safety Administration (NHTSA), which aims to "save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement"
   - The Federal Transit Administration, which oversees most aspects of the nation's mass transit systems; however, it is outside of the scope of this chapter since it deals with passenger transportation
   - The Transportation Security Administration (TSA), which administers the sky marshal program that was reinstituted after 9/11/2001
2. Refer to FHWA's Comprehensive Truck Size and Weight Study Executive Summary, October 2000.
3. Weight $= 500 \times \{[(\text{Length in Feet between Axles} \times \text{Number of Axles})/(\text{Number of Axles} - 1)] + (12 \times \text{Number of Axles}) + 36\}$
4. The Final Rule was issued on April 22, 2005.
5. The Act is formally called the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act, hence the acronym USA PATRIOT.
6. For example, Railroad Antitrust and Competition Acts HB 3318 and HB 2047.
7. For a reference on cost differentials, see the Maritime Cabotage Task Force's Post Hearing Brief on the Economic Effects of Significant U.S. Import Restraints, 1995.
8. The last operating differential subsidy expired in 2001, and the Ocean Shipping Reform Act of 1998 (OSRA), also called the Shipping Act of 1998, allowed confidential service contracts between shippers and ocean common carriers. OSRA concealed from public view most details of the contracts except the origin and destination port ranges, the commodities involved, the minimum volumes, and the duration of contracts. Confidential contracts with shippers decreased the influence of conferences, trade-based shipping cartels that had previously fixed the terms of engagement with shippers.
9. American President Companies merged with Neptune Orient Lines Ltd, a Singapore-owned and -operated line, in 1997, and SeaLand was bought by Maersk in 1999.
10. (1) College Park Airport (CGS), (2) Potomac Airfield (VKX), and (3) Washington Executive/Hyde Field (W32).

PART 7

FINANCIAL SERVICES GOVERNANCE

CHAPTER 41

FINANCIAL SERVICES REGULATION AND CORPORATE GOVERNANCE

Dennis Cox

41.1 THE HISTORY OF FINANCIAL SERVICES REGULATION

The financial services industry has been at the center of regulation for centuries. Given this level of experience in compliance and regulation, it would be nice to be able to say that regulation was generally well thought through and fit for purpose. Unfortunately, this is generally not the case.

Regulation within financial services is generally the result of a knee-jerk reaction to an acknowledged problem that is perceived to be facing the industry. There are generally two forms of financial regulation; that enforced by legal sanction and that imposed with the general support of the regulated, but without sanction—the so-called self-regulation option.

What tends to happen is that the industry perceives some kind of issue and then works as a group to design some form of voluntary standard that the market is willing to accept. This normally works fine until such time as something goes wrong; then the legislature tends to think that legislation is the only reliable option. So we tend to get these irrational movements in financial regulation, often designed within silos and rarely representing joined-up writing. I will explain this in more detail later.

41.2 INTERNATIONAL REGULATION

The Bank for International Settlements (BIS), based in Basel, Switzerland, was originally set up by a group of bank governors. At that time central banks were often the regulators of the banks within their bailiwicks. The Bank for International Settlements is therefore not a bank and its pronouncements do not have legal force. Local regulators need to take the rules promulgated from Basel and implement them within the local regulatory environment.

In the case of the European Union, this normally means some form of new directive being issued by Brussels. These directives must also be transposed into local legislation. So if you are a UK-based institution, you need to look at the regulations that are coming from Basel and also those coming from Brussels. It would be nice to say that these were always consistent. Mind you, it would be nice to say a lot of things!

The idea of the BIS, and the rules to which most countries in the world have signed up, is to create a so-called level playing field. The basic proposition that one man's regulation is another man's regulatory opportunity leads to the objective that if all countries had the same set of regulations, then international business would operate more effectively.

At the heart of the regulatory structure is the idea that banks should hold a certain level of capital to provide a level of protection against failure. The three-pillar approach to regulation therefore prescribes capital calculations with pillar one, leaving other matters for pillar two and disclosure for pillar three. The latest version of the Basel Accord for the first time requires internationally active banks to hold capital for operational risk, albeit that the majority of pillar one capital is still calculated in respect to credit and market risk.

So what is the capital for? The basic tenet is that around 9 percent is required for capital maintenance, with the regulators adding a few percentage points to cover such other matters as reputational risk, liquidity risk, and strategic risk. The new Accord will not, on balance, change the general amount of capital in the system, although individual firms will find that their capital requirements may change. Why "may"? Because it still remains a regulatory construct as to the level of capital that is required, so the regulators are still likely to be loath to allow a firm to reduce the level of capital that is required.

The idea is that as banks move to more advanced calculations with respect to both credit risk and operational risk, they gain an advantage in terms of a reduction in the capital calculation. Well, that is the principle. My concern remains that as a bank achieves a lower calculation within pillar one, then the regulators may just increase the capital charge within pillar two.

41.3 WHAT IS THE POINT OF REGULATORY CAPITAL?

The general view from the regulators is that capital maintenance rules are there to protect the public. No similar rules exist in other industries, so why are they

required within banking? The concern is that banks have a fiduciary responsibility and therefore need to keep capital to make sure that any depositors can lend their precious funds to the bank with impunity.

Of course life is not like that. When a bank really fails it tends to munch through all of its regulatory capital and keeps on going. It is only a bailout from a government, central bank, or independent third party that will solve the problem. In such cases the depositors and shareholders tend to lose out. No, capital cannot protect against this form of cataclysmic failure—rather, insurance of some form would cope much better. That is why most countries have some form of deposit protection scheme in operation to provide some level of support to depositors, particularly at the lower levels.

So capital is poor at protecting the individual investor. Another option put forward is that the market does not want the failure of one institution to have a significant impact on another institution, potentially leading to its failure. This is the thought that the capital held will act as a first loss buffer and protect the market. Once again the history of banking regulation puts this idea into question. If there is a problem at a bank that becomes public, the depositors and international counterparties all start to close out their positions with the firm. This tends to lead to the failure of the institution, which subsequently defaults on its obligations. Under this type of closeout scenario, the losses within the institution tend to multiply.

First there is the original event that caused the loss, perhaps a fraud or an error. Then there is the liquidity mismatch that occurs that will need to be covered by some form of reserve line of funding, which will certainly be more expensive. Finally there are also losses incurred due to the bank defaulting on its obligations and also needing to close out transactions to meet these liquidity requirements, together with the loss of reputation. Consequently, the actual loss to the bank is likely to be a multiple of the original event. This is why when an event occurs at a publicly quoted bank the reduction in the share price is a multiple of the actual event losses originally incurred.

What you tend to see is that the losses actually cascade through the system. This does not only need to be the case with the failure of a bank such as Barings or the Bank of Credit and Commerce International (BCCI). Rather, it could be the result of the failure of a large corporation or hedge fund, for example Enron or Long-Term Capital Management. The losses act a bit like lightning, trying to find the shortest route to the ground and creating havoc in their wake. The failure of one institution, say an investment bank, may cause problems at other investment banks that are closely related to it through business activity. If the market believes this occurs, then it will ensure it does occur through the operation of the herd mentality—and the second firm goes into stress. The failure of these two institutions can then cause others to fail, and the problem continues to multiply.

So the conclusion is that the capital is not sufficient to really protect the market. Better risk management is the approach to adopt, and this is also included within pillar two of the Accord.

So if it is not to protect the depositor or the market, what is the real point of capital maintenance? The only party that actually is supported by the maintenance of capital in accordance with international rules is the regulator. As such regulatory capital is a regulatory construct and should be recognized as such.

41.4 HOW MUCH REGULATORY CAPITAL IS REQUIRED?

Companies maintain capital regardless of the industry they are in to provide sufficient liquidity to maintain current operations and flexibility to enable investment and other corporate activities to take place. As such, banks are no different and would certainly maintain capital to the level that management considers appropriate even in the absence of the rules that are currently available. The rules come up with a particular number as base—around 9 percent. What is the basis for this? Should the figure be 5 percent or 20 percent? Quite frankly, we have no idea what would be the impact on the global market of coming up with a different capital figure to calculate. What the Accord does is calculate the same figure with no rational basis in a way that is more risk sensitive. Perhaps this is useful, but it could also be considered rather preposterous.

But matters are worse. In the Accord, credit risk capital is calculated based on historic loss experience and current exposures. Market risk capital is primarily based on a calculation that starts with the mark-to-market value of a series of extant positions. Operational risk is rather different—for the basic and standardized approaches it is based rather illogically on profits. For the advanced approach it is a future-looking loss distribution approach. While we are not really going into full detail on what all of this means, the basic problem is that these three modeling approaches are inconsistent.

Readers of *Mathematics of Banking and Finance* by Dennis Cox and Michael Cox (John Wiley & Sons, 2006) will note that we state quite clearly that modeling approaches need to be consistent. In the Basel Accord they are not, which means that there is no mathematical rigor to adding these three values together. Again, it is a regulatory construct with limited intellectual property.

The best thing about the Accord is that it has raised the idea that banks need to undertake a higher level of risk management, understanding the risks that they are running so that proper management oversight can take place.

41.5 OTHER FINANCIAL REGULATION

Have you tried to purchase something like a unit trust or a pension from a bank recently? The regulations now require the bank to go through a mass of detail to ensure that you really understand the risks of the product you are purchasing. I was discussing this with a journalist a few weeks ago who had recently purchased such an investment. Had he received a package of information to

explain the product? Yes, he had, he replied. Had he read them, I asked. No, he responded, they were too detailed and too boring—anyway, why would the bank sell him something that was unsuitable? Financial services regulation has moved to an extent that mere mortals without a degree in financial literacy are almost unable to read the statements that they receive, let alone the "reasons why" letters and additional literature that regulations require the individual to receive.

Clarity has been lost, and also there has been a significant impact on the availability and cost of truly independent advice available to the individual. But the regulators can check that everything is done in accordance with the rules and believe that this is somehow improving things. I have news for them: The unscrupulous do not tend to follow the rules. They will appear to be doing what the regulators require, while also acting inappropriately to the detriment of the investors and the market.

What we are seeing is a growth in regulation, driven in Europe by the European Union, leading to ever more complex documentation and regulation. This puts additional costs onto the bank while at the same time providing the customer with limited protection. I regret to say that the growth in compliance rules and regulations is likely to continue—once you have regulators, they are certain to want to change the rules as often as possible to make sure that if anything goes wrong it was always due to a prior regime. This may be a little tongue-in-cheek, but I am sure you get my drift.

The discussions in the United States are even more arcane. The reluctance of the U.S. regulators to embrace Basel regulation is a disappointment, and their reluctance to part from 15-year-old flawed capital calculations even sadder. I can see no reason why all U.S. financial institutions should not implement the Basel Accord in full, just as their UK counterparts are doing. I believe the regulators in this case are doing a disservice to their own industry, and their suggestion that the world should adopt the 1991 leverage ratio—a construct that takes no notice of risk—is at best bizarre.

41.6 MONEY LAUNDERING DETERRENCE

Another major area of financial regulation surrounds money laundering. The PATRIOT Act in the United States, the directives in Europe, and the Weisberg principles globally, together with comments from the BIS, have resulted in rules and regulations being implemented almost globally.

The Financial Action Task Force (FATF) was formed to ensure that countries implemented money laundering deterrence regimes, and therefore noncompliant countries would be penalized by the banking community needing to undertake additional procedures with regard to transactions with such a country. This sounds great—but at present there is only one country on the list: the major center of money laundering that is Nauru. I jest, of course, but that does mean that as a list of countries to look out for, FATF is no longer very useful.

Money laundering deterrence started with trying to stop drug trafficking and terrorist financing, but has expanded, particularly in the UK, into becoming an all-crime offense. As such, theft is clearly included, together with extortion and tax evasion. With the UK Financial Services Authority having the detection of serious crime as an objective of its regulation, the UK and global regulators are increasingly focused on anti–money laundering.

Of course, nobody believes that increasing money laundering regulation actually results in a reduction in crime. Theft, drug trafficking, terrorism, and tax evasion are all growth industries. What the regulation actually does is to make life difficult for regular people.

I will give an example under the rules that existed in the UK last year. At that time if you wanted to open a bank account you required two pieces of documentation, for example a passport and a driving license or utility bill. In my office we had a young man working for us who did not have a driving license and since he lived with his parents, no utility bills. He had a bank account with a UK High Street bank and wished to open an additional deposit account. He duly produced his passport and a copy of his bank statement as secondary evidence. The bank rejected the statement since it came from them and requested a driving license or utility bill, which he was unable to provide.

A simple solution was then suggested. Go to a competitor and use your passport and the bank statement to open a new bank account. You just need to deposit £1 and then you can use the statement from that bank to open the new account here. That is regulation just gone mad.

Of course it makes sense for a bank to understand its clients and record the source of funds. If nothing else, this will enable the bankers to think about the products that they should be selling to the customer as opposed to those that are actually currently being sold. The fight against organized crime is also assisted by banks retaining sufficient information to enable the complex web of transactions to be identified. However, many of the rules are really just inconveniencing real customers, rather than money launderers. One thing that can be said with certainty is that the money launderer normally has perfect documents and will provide the bank with everything that it requires. They will even look like their passports. It is mere mortals like you and me who do not have or forget to bring the right paperwork and don't look like their passports except in a bad light if you squint and have a good imagination.

41.7 BANKING AND THE ENVIRONMENT

It is often said that banks need to consider the special position that they hold in the community and act accordingly. They must ensure that there is no social exclusion and that no part of the community is disadvantaged. Many operate programs that assist the communities in various ways, mostly because this is all good public relations (PR). Others take a deliberate approach to being environmentally sound and disclose their policies in their financial reports. The real question is whether

or to what extent this is the role of the banks. In the UK when a bank reports its profits there is normally an outcry about the level of profits made. That most of these profits are not made in the UK and that it is these profits that enable the bank to maintain capital and lending rates is not often covered to the same extent.

There is a lot of difference between acting ethically, which all banks should do, and being environmentally friendly. Should a bank refuse to take a tobacco industry or oil industry client just because they could be seen as not environmentally friendly? What about lending to a leader of a country that might at some later stage be seen as being unethical? While the idea appears initially preposterous, there is no doubt that such discussions are now taking place in many banks. In my opinion, banks are often left in an uncomfortable position, effectively being damned if they do and damned if they do not.

41.8 THE FUTURE OF BANKING REGULATION

I believe that financial regulation will continue to develop and that this will extend beyond banking to all areas of the industry, as is currently the case in the UK. Even the United States will eventually fall into line and accept global regulatory and compliance standards or will find its banks trading with a disadvantage.

The Basel Accord, which will remain the pinnacle regulation, will be amended on a regular basis. First (2009), they will sort out the anomalies within credit risk; then they will bring liquidity risk clearly into pillar one while clarifying other elements of operational risk in a far more explicit and restrictive way. The next update (2011) to the Accord will bring strategic risk into pillar one, with reputational risk following in a later update (2014). The argument for excluding them from pillar one (that they are too difficult to calculate) is really rather weak. Just because something is difficult to calculate does not mean that it goes away!

Then the big change will follow. By 2020 a completely different basis will be used that looks at risk on a consistent basis across all risk types and actually comes up with a calculation that makes sense. Pillar two will then become the procedures that a financial services firm should implement at a minimum to provide adequate levels of control, with disclosure in pillar three. And the strangest thing of all is that we could do it all now if we had either the imagination or the will to do so.

CHAPTER 42

INSURANCE INDUSTRY AND SOLVENCY II

Anthony Tarantino, PhD

42.1 INTRODUCTION

In banking think capital adequacy; in insurance think solvency. The concepts are closely related, and both are behind global initiatives that will transform the financial services industry.

Capital adequacy sets standards for the minimum level of a bank's equity in relationship with its assets as set by the Bank for International Settlements (BIS) through its Basel Committee. The new accords are known as Basel II. Capital adequacy measures financial strength and requires banks to have capital equal to 8 percent of their assets. The European Union's Capital Adequacy Directive established minimum capital requirements in the financial services industry and has been in effect since 1996. The Basel II capital accords go into effect in the next few years in the EU and other countries.

Solvency is used in the insurance industry to measure an insurer's ability to pay its debts with available cash. Solvency has not traditionally referred to a calculation but rather been treated as a statement of fact—you are either solvent or you are not. Financial ratios are now being applied to predict solvency problems. Solvency is different from profitability, which is the ability of a company to earn

a profit. A company can make a profit without being solvent and be solvent and lose money. The game is over (bankrupt) when a company is both unprofitable and insolvent. The European Commission (EC)'s Financial Services Action Plan (FSAP) developed a new solvency regime known as Solvency II. The EC has relied on the International Association of Insurance Supervisors (IAIS) to provide the guidance around Solvency II, which is designed to replace the 30-year-old Solvency I guidance by 2010 to 2011. It is intended to provide a more quantitative and qualitative risk-based focus to minimum capital requirements and supervision.

The IAIS was established in 1994 and represents insurance regulators and supervisors of over 180 jurisdictions in more than 130 countries, constituting 97 percent of insurance premiums in the world. The IAIS objectives include:

- Contribute to improved supervision of the insurance industry on a domestic and international level in order to maintain efficient, fair, safe, and stable insurance markets for the benefit and protection of policyholders.
- Promote the development of well-regarded insurance markets.
- Contribute to global financial stability.[1]

Solvency Foundations. In 2005, the IAIS published a series of guidance white papers that lay the foundation for an improved insurance solvency framework and infrastructure. The IAIS objectives are to improve industry supervision by:

- Enhancing risk and solvency management for insurers, reinsurers, and related financial groups
- Enhancing financial transparency and cross-border comparative analytics
- Promoting a level playing field across the insurance industry
- Promoting international collaboration and cooperation
- Reducing unwarranted regulatory arbitrage
- Increasing government, investor, and consumer confidence in the insurance industry
- Enhancing improved industry efficiency and productivity[2]

Solvency Preconditions. The IAIS describes the preconditional requirements for an effective solvency framework as creating an environment that has:

- Industry-wide and regionally wide policies, procedures, and standards that are clearly defined, understood, and accepted
- Mature and effective financial market infrastructure
- Effective and efficient financial markets with easy access to pertinent information
- Adequate enforcement powers and a regulatory staff with the proper charter
- Whistle-blower and other legal protections

- Operational independence to avoid conflicts of interest and maintain segregation of duties
- Clear accountability and transparency in regulatory functions and powers
- A highly professional and ethical staff
- The ability to maintain confidentiality to avoid revealing competitive information[3]

Solvency Framework. With these preconditions in place, a three-block or -category solvency framework is possible to address capital adequacy, governance, and market conduct:

1. *Capital adequacy.* This includes solvency and capital adequacy, methodology and technology to calculate capital adequacy, technology to support financial calculations, types of capital, investments, and financial reporting and disclosure.
2. *Governance.* This includes corporate board and management governance, tone at the top to assure adequate internal controls, and risk management to comply with laws, regulations, and standards while meeting shareholder and other stakeholder expectations.
3. *Market conduct.* This includes customer relationship management (CRM) in the selling and managing of insurance policies, as well as the issuer's integrity in its conduct as an institutional investor. This also requires financial disclosure of relevant information to company stakeholders, the marketplace, and customers.[4]

Solvency Infrastructure. The IAIS also describes several elements of the needed infrastructure required as to preconditions, finance, governance, market conduct, supervisory assessment and intervention, and disclosure:[5]

Preconditions. Insurers should assess and manage risks, set regulatory financial requirements, and, if need be, require the holding of additional capital and/or reduce risks so assets meet minimum requirements.

Financial requirements

- Regulatory financial requirements should be risk sensitive and align risk management, regulations, and policyholder interests.
- Risk management needs to address all types of potential risks—legal, underwriting, reputational, market, credit, liquidly, and operational.
- The interdependence among capital requirements, capital resources, assets, and, liabilities must be recognized in a total balance sheet approach to solvency.
- The vast majority of insurance obligations should be met by the insurer through the settlement of insurance contracts, and not by transferring the obligations to another insurer.
- Portfolios should be evaluated using a consistent, market-based approach, not using the individual policyholder holding the portfolio.

- A risk margin calculation should be made for the cost of meeting the policy obligations. The calibration provides that the technical provision valuation is equivalent to the value that an insurer would need to cover in order to assume the obligation.
- Regulatory capital needs to be adequate to cover policy claims and other obligations in the midst of adverse economic conditions.
- The calibration of capital requirements should assure that assets will exceed technical provisions during times of adversity with a defined safety level over a specified time range.
- Risk management should be aligned with market assumptions and change according to changes in market conditions.
- The risk reflected by additional risk exposure that is outside of the policy portfolio should be covered in additional capital.

Governance. Insurers should maintain corporate governance policies, procedures, and standards that support good risk management while obeying all laws and regulations and meeting stakeholder expectations. This is the foundation to any effective solvency regime.

Market conduct. Insurers should practice sound, ethical, and transparent market conduct policies and procedures.

Supervisory assessment and intervention. Solvency controls should be in place that create varying degrees of timely intervention depending on the nature of the control issue.

Disclosure. Disclosure policies and practices should define the type and level of public information to promote market discipline and corporate governance.

(a) SOLVENCY I TO SOLVENCY II. Solvency II creates major challenges for the insurance industry with a regime that is much more demanding than the old Solvency I. Capital markets are demanding greater stability and clarity in the measurement of solvency. While improving solvency requirements, the EC believes that the rules for banks and insurers should be harmonized in that many of their product offerings are overlapping and many European banks offer insurance products—Solvency II has been referred to as Basel for insurers.

Solvency II is part of a global drive to strengthen and harmonize financial services standards and diligence. The public face of the process is to improve consumer protection, but the underlying thrust is to improve market stability and confidence—avoiding the painful crisis cycles of the past. Solvency II calls for a comprehensive regulatory framework intentionally modeled after the Basel II accords. The EC's Solvency II initiative will reshape the insurance industry in the EU and eventually on a global basis. Like its banking counterpart, Basel II, it will compel a major consolidation in the industry as smaller players struggle to meet much more stringent regulatory requirements. A survey by Conning Research and Consulting indicates merger activity at the highest level since 2001, with no signs of a slowdown.[6]

Solvency II takes a three-pillar approach similar to the three-pillar approach that Basel II applies to the banking industry.[7] The three pillars can be summarized:

Pillar one: Minimum capital requirements. The first pillar is about improving insurer solvency capital management. It includes both a target and minimum solvency capital requirement. The minimum solvency capital depends on the dollar value of polices written and is fairly straightforward to calculate. The calculation takes a risk-based approach around assets, liabilities, and underwriting information. Target solvency capital is typically the same as economic risk capital needed to cover disaster scenarios. There will be EU-wide model target solvency capital calculations, but each member nation will be able to modify the model somewhat.

Pillar two: Supervisory review process. The second pillar is about insurer supervisors monitoring the amount of their existing capital. This will include improving cooperation and standardization among regulatory authorities in each of the member states. It will also include an assessment of internal controls, risk management, and segregation of duties, stress testing of IT infrastructure and systems, senior management capabilities, and the balance between assets and liabilities.

Pillar three: Enhanced disclosure and market discipline. The third pillar is about improving the public's access to the company's financial and risk management information. This includes efforts to comply with accepted best practice frameworks.

Each of the three pillars of Solvency II will be affected by the risks that an insurer writes. The minimum capital required by pillar one will reflect the risks the insurer runs, and pillar two encourages a proactive attitude to the management of those risks. Pillar three will allow observers to compare the approach that different insurers are taking to risk. For instance, an insurer with a greater risk appetite should carry a higher capital requirement for the same credit rating.

Solvency II requires the following risk and control environment:

- An obligation to introduce an early risk warning system
- The presentation of future risks in a status report
- Periodic audits by company accountants
- The creation of internal control systems initiated by the Federal Financial Services Supervisory Authority
- A risk strategy with the following requirements:
    - Creating an effective reporting system
    - Installing early warning and monitoring tools
    - Changing existing internal risk management processes so they can be measured against the new requirements (pillar two)

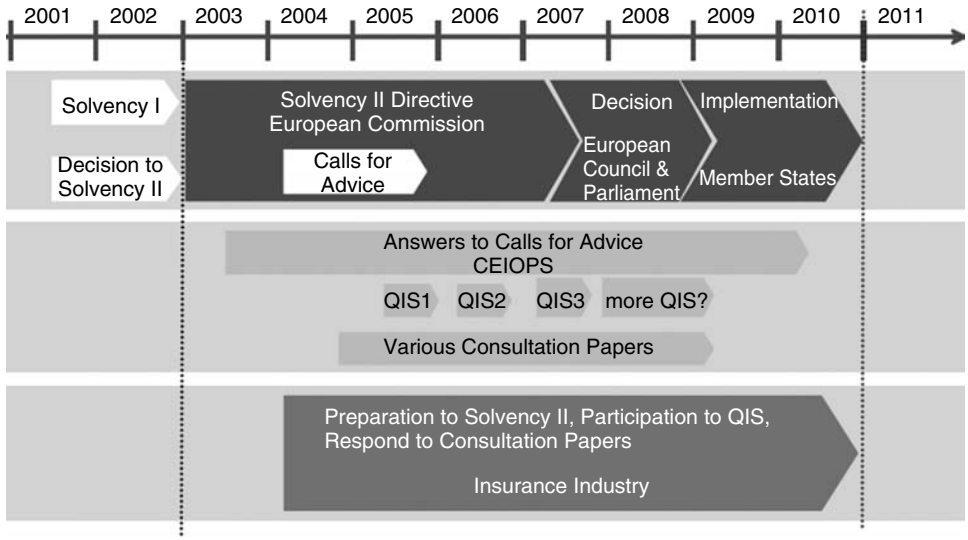


EXHIBIT 42.1 TIME LINE OF THE SOLVENCY II PROCESS

Solvency II Time Lines. The European Insurance and Reinsurance Federation (CEA) has created a time line of the Solvency II process as shown in Exhibit 42.1.[8]

(b) BASEL I TO BASEL II. In 2004, the central bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries published a new framework for capital adequacy called "The International Convergence of Capital Measurement and Capital Standards: A Revised Framework." This is commonly known as Basel II since the meetings took place in Basel, Switzerland. The first Basel accord (Basel I), published in 1988, set standards for capital requirements because banking regulators well understood that weaknesses in internal controls presented major risks to banking on a global level.[9]

The Basel II framework builds on the 1988 accord, setting out the details for adopting more risk-sensitive minimum capital requirements for banking organizations and including:

- A framework for banks to assess the adequacy of their capital and the adequacy to support their risks
- A framework for banks to strengthen market discipline by enhancing the transparency in banks' financial reporting

The Basel Committee has made the new framework, including the advanced measurement approach (AMA), available for implementation in member jurisdictions.

Pillar	Solvency II	Basel II

One	**Minimum Capital Requirements:**
	• Target and minimum solvency capital requirement
	• Minimum solvency capital depends on the dollar value of policies written
	• Calculation takes a risk-based approach around assets, liabilities, and underwriting information
	• Target solvency capital typically the same as economic risk capital to cover disaster scenarios
		Minimum Capital Requirements:
		• Minimum acceptable capital levels
		• Internal ratings-based (IRB) approach to determining credit risk charge
		• Explicit treatment of operational event risk in capital calculations
		• Computation of capital charge
		• Credit risk
		  ○ Three approaches with increasing risk sensitivity
		  ○ Recognition of credit risk mitigation
		  ○ Operational risk
		  ○ Three approaches with increasing risk sensitivity
		  ○ Trading book

Two	**Supervisory Review Process:**
	• Insurer supervisors monitoring the amount of their existing capital
	• Improving cooperation and standardization among regulatory authorities in each of the member states
	• Assessment of internal controls, risk management, and segregation of duties; stress testing of IT infrastructure and systems, senior management capabilities, and the balance between assets and liabilities
		Supervisory Review Process:
		• Banks assess their own solvency relative to risk profile
		• Supervisors review bank's assessments and capital strategies
		• Banks hold capital in excess of minimum requirements
		• Regulators intervence at an early stage if capital levels deteriorate
		• Perspective of supervisor
		  ○ Four key principles of supervisory review
		  ○ Principle of double proportionality
		  ○ Specific issues under supervisory review process

Three	**Disclosure and Market Discipline:** • Improved public access to the insurer's financial and risk management information • Efforts to comply with accepted best practice frameworks	**Disclosure and Market Discipline:** • Increased disclosure of capital structure • Increased disclosure of risk measurement and management practices • Increased disclosure of risk profile • Increased disclosure of capital adequacy • Perspective of market: qualitative and quantitative requests, regulatory capital, capital structure, risk exposures, risk assessment, scope of consolidation

EXHIBIT 42.2 THREE PILLARS OF SOLVENCY II AND BASEL II

(c) COMMON ELEMENTS OF BASEL II AND SOLVENCY II. Basel II and Solvency II will require banks and insurers to rethink their existing risk management strategies in that many of them do not have systems to quantify and mitigate risks. Both call for enhanced internal controls, including risk management, as a means to promote transparency in financial reporting. Unlike punitive systems, such as the U.S. Sarbanes-Oxley Act, the two accords would reward banks and insurers for improvements in risk management with lower capital and insurance rates. Improved rating agency scores and evaluations will make their stocks more attractive in the marketplace.

As mentioned, both Solvency II and Basel II take a three-pillar approach that is similar by design. The parallels between the two accords are growing in importance as the distinctions continue to blur between various types of financial service providers. The next generations of Basel and Solvency will bring the two accords into even closer alignment. Exhibit 42.2 shows a simple mapping of the three pillars of Solvency II and Basel II.

42.2 VALUING INSURANCE LIABILITIES

Market Consistent Value of Liabilities (MVL). The most recent draft of the Solvency II framework was due in July 2007 and includes a definition of the market consistent value of liabilities (MVL), which is the basis for determining solvency requirements in the insurance industry.

Market Value Margin (MVM). A key area in this calculation is the method for quantifying the market value margin (MVM) for nonhedgeable risks. While a company could eliminate or mitigate much of its risk exposure for hedgeable risks by purchasing hedging instruments or transferring risk to a counterparty, nonhedgeable risks require a MVM calculation. These are some of the options for calculating MVM:

- *Cost of capital approach.* The cost of capital approach requires a best estimate for reserves based on realistic cash flow projections into future periods. In addition, a market value margin needs to be calculated as capital cost to cover regulatory risk capital in future years. Hedgeable risks could be valued directly using current market data.
- *Scenario-based approach.* The scenario approach requires a liability's market value to be based on cash flows, which are projected into future periods using a variety of long-term stress scenarios. Unlike the capital approach, the scenario approach requires the retention of different data sets for stress scenarios.
- *Percentile approach.* This approach would use a stochastic and future projection of cash flows. It may require the data system to interface an actuarial software application, which is based on points of a model rather than individual contracts. This would require the storage of statistical data. The percentile approach is based on ensuring that risks can be covered at an appropriate level of confidence, typically 75 percent.

42.3 SOLVENCY CAPITAL AND MINIMUM CAPITAL REQUIREMENTS

A key requirement of the solvency regime under pillar one is the calculation of solvency capital requirements (SCRs) and minimum capital requirements (MCRs). Solvency II provides two methods to calculate SCRs; the internal model is more appropriate for larger firms, whereas the standard approach is more appropriate for small to midsize firms. The internal model system will require more sophistication and resources. If the experience of the banking industry is repeated, insurers may find credit agencies driving their decisions ahead of regulators and in the direction of the internal model approach in order to receive the most favorable ratings.

Internal Models. Large insurers routinely operate sophisticated internal models to reflect the individual characteristics of their liabilities, and suitably validated, these can be used to calculate SCRs. Solvency II will be implemented under the Lamfalussy process, so directives will remain fairly high level with the details to be worked out at a lower level. If the history of the banking industry under Basel II repeats itself, the ability to provide years of very clean loss data may present major challenges in building viable internal models.

Standard Approach. As in banking, small and medium-sized companies face challenges in developing internal models. Solvency II permits the use of the standard approach, which is designed to achieve similar results to the internal model approach. Because of its lower level of precision, the standard approach includes more conservatism and higher costs for those who use it. The attraction is that someone else has done much of the work and implementation costs are lower than with the internal model approach. However, no two insurance companies are the same, with variations in control processes and risk appetites. A company applying the wrong standardized model could pay a big capital premium on one side of a mistake or be undercapitalized on the other side of a mistake.

42.4 OPERATIONAL RISK MANAGEMENT

The International Association of Insurance Supervisors defines operational risk as "the risk arising from failure of systems, internal procedures and controls leading to financial loss. Operational risk also includes custody risk."[10]

The EU Directive 2006/48/EC and Basel II provide for three approaches to operational risk that are likely to be applied to the insurance industry:[11]

1. *Basic indicator approach (BIA).* A simple percentage of net income is set as the level of regulatory capital required.
2. *The standardized approach (TSA).* Individual percentage requirements are applied to different lines of business and the result is then totaled. The TSA will likely be applied to insurers lacking the resources and sophistication to use internal modeling.
3. *Advanced measurement approach (AMA).* Models, data sources, and statistical techniques are used to develop a more relevant quantification of the operational risk facing an individual company.

Pillar II of Solvency II for insurers is also likely to require an assessment of operational risk through the use of either standard or internal models. This has increased interest in the 1992 Committee of Sponsoring Organizations (COSO) framework and its 2004 update known as Enterprise Risk Management (ERM). This is a mixed blessing. Both COSO frameworks filled a much-needed demand for risk management, but neither provides an adequate means to quantify risk. The insurance industry would do well to compare notes carefully with the experiences in the United States and the banking industry. The U.S. experience under the Sarbanes-Oxley Act's Section 404 and its companion audit standards created a very expensive overreaction to risk management, all the while following the COSO framework. Banking took a more practical approach using quantitative methods to rationalize risk.

The U.S. and banking industry experience would also indicate the insurance industry can expect the following issues and problems:

- A shortage of quantified risk managers and analysts
- Role confusion in separating risk from compliance management
- Difficulty in providing historical risk-related data that is consistent and cleansed
- Difficulty in understanding what is expected in risk management
- Credit agencies continuing to raise the bar for risk management ahead of regulations and giving little latitude to smaller firms

Under Solvency II, firms will need to demonstrate the following around risk management:

- The framework is the basis for a dynamic process.
- Risk information flows both up and down the organization.
- The risk assessment process has a direct influence on decision making and management actions.
- There is transparency around the decision making process and the role of risk.
- There is a systematic tracking of operational risk data, which includes material losses by business lines and potentially near-loss data.
- An integrated risk assessment system exists that is responsive to the insurer's interests.

42.5 ISSUES FACING INSURERS IN IMPROVING OPERATIONAL RISK

These are some of the issues insurers will face in improving operational risk. There are parallels to the issues bankers face.

- Few insurers utilize operational risk capital allocation and policy in making strategic decisions.
- Few insurers utilize robust quantitative and statistical methodologies in measuring operational risk and the capital provisions it implies.

- Many do not use any internal or external historical data to estimate operational risk.
- Many will struggle in obtaining the benefits of the AMA because they lack adequate and consistent internal loss data.
- Many insurers are carrying more operational risk and capital than they need, but lack the quantitative tools, experience, and executive sponsorship to improve the situation.

42.6 ISSUES FACING INSURERS IN IMPROVING DATA INTEGRITY AND RETENTION

As with Basel II, Solvency II will substantially increase data accuracy, retention, and retrieval requirements as both regimes require the use of multiple years of internal and external loss data in order to calculate regulatory capital levels. This includes data to support quantitative and qualitative risk management techniques, which will make greater demands on data accuracy than either banking or insurance has ever experienced.

The insurance industry has conducted a series of Quantitative Impact Studies (QISs) to test the current state of the insurance industry to calculate solvency capital requirements (SCRs). These studies suggest many insurers will struggle in such areas as:

- Accurately capturing 15 years of historical data (net combined ratios) may be a challenge.
- Predicting a level of confidence for a once in 200 years event—a Katrina or a tsunami—may be difficult.
- Differences in tax laws across jurisdictions may present problems in estimating risks based directly on history.
- The reliance on data histories may make it necessary to normalize historical data according to a fixed standard in order to be meaningful (e.g., while cars are more expensive and thus more costly to repair, improved safety features are reducing injuries during accidents; therefore, historical data cannot be simply applied without normalizing it—not a simple task).
- In many cultures admitting failures is very difficult and the norm is to hide failures; therefore, collecting risk data will be very challenging.

42.7 ISSUES FACING INSURERS MEETING IFRS AND SOLVENCY II

A joint study by the Ecoledes hautes etudes commerciales du nord (EDHEC) Risk and Asset Management Research Center and the EDHEC Financial Analysis and Accounting Research Center argues that there are fundamental contradictions between Solvency II and the new International Financial Reporting Standards (IFRS) being adopted across the EU and much of the rest of the world.[12] The IFRS is a principles-based approach to generally accepted accounting principles

(GAAP). Over 7,000 EU companies now report their financials using the IFRS, which is replacing a wide variety of national/local GAAPs. The IFRS is also gaining global acceptance, with active transition programs underway in most nations with the notable exception of the United States, which uses a rules-based GAAP.

Specifically, the study argues that improved risk management proposed by Solvency II will conflict with certain provisions of the IFRS. Under the IFRS, insurers that reduce risk by applying good asset-liability management (ALM) may be penalized. This is caused by increases in volatility from an accounting perspective, even if does not increase volatility in reality. In short, Solvency II will require firms to do a better job of exposing risks, and the exposure can harm a company's bottom line. Solvency II seeks improved management and measurement of risks associated with assets and liabilities. The conflict with IFRS comes in the old adage that ignorance is bliss. Those who do a poor job of identifying risks are rewarded in their financial reporting—until something goes wrong, of course. Those who do a better job of identifying risks are punished for admitting that greater levels of risk exist.

While the study makes a very valid point about the dilemma, it is less clear as to why the IFRS is more harmful than other accounting practices. This dilemma should exist in any GAAP. U.S. banks now preparing for their parallel year under Basel II will face the issue of having to make references to their going-to state under the advanced measurement approach (AMA) of risk management. It is likely to show that banks are less profitable than currently reported and therefore need greater regulatory capital under the more rigorous regime of the AMA.

The short and simplistic answer to the Solvency II/IFRS dilemma is for insurers to improve their risk management and measurement and ultimately lower their risk exposures. While insurers may see their financials suffer in the transition, regulators, rating agencies, and the market will reward those that aggressively adopt Solvency II risk management protocols.

42.8 THE LAMFALUSSY PROCESS IN DEPLOYING SOLVENCY II

The three pillars of Solvency II are to be deployed via what is known as the Lamfalussy process or structure. The Lamfalussy process is used in the EU to regulate the financial services industry. It was developed in 2001 and named after Alexandre Lamfalussy, the chair of the EU advisory committee that created it. It is made up of four levels, each of which focuses on a specific stage of the implementation of legislation.

Level One: Legislation is enacted by the European Parliament and the Council of the European Union. This establishes an overarching umbrella of core values behind the legislation.

Level Two: Sector-specific regulators and committees advise on legislative details, and then create nation-specific laws.

Level Three: Each nation's regulators collaborate with each other to coordinate and harmonize new regulations.

Level Four: Each nation creates the resources and organization needed to assure compliance with the new laws and regulations.

The Lamfalussy process has proven to be effective over the traditional legislative process by providing more consistency in interpretation, convergence, and quality of legislation. A good example of this is the creation of the Markets in Financial Instruments Directive (MFID).[13]

This Lamfalussy process translates into a fairly high-level guidance with the details left to cooperative efforts among the national governments. The CEA provides a table of the four levels of the Lamfalussy process for Solvency II, as shown in Exhibit 42.3.[14]

The European Commission calls for three waves of advice as to the framework to be deployed by the fourth level of the Lamfalussy process, as shown in Exhibit 42.4.[15]

Level	What Does It Do?	What Does It Include?	Who Develops?	Who Decides?
Level 1	Solvency II Directives	Overall framework principles	European Commission	European Parliament, European Council
Level 2	Implementing Measures	Detailed implementation measures	European Commission	European Insurance and Occupational Pensions Committee (EIOPC)
Level 3	Supervisory Standards	Guidelines to enhance supervisory convergence	Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS)	Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS)
Level 4	Evaluation	Monitoring compliance and enforcement	European Commission	European Commission

EXHIBIT 42.3 FOUR LEVELS OF LAMFALUSSY PROCESS FOR SOLVENCY II

Pillar One—2nd Wave	Pillar Two—1st Wave	Pillar Three—3rd Wave
Technical Provisions in Life Assurance	Internal Control and Risk Management	Eligible Elements to Cover Capital Requirements
Technical Provisions in Non-Life Insurance	Supervisory Review Process—General	Cooperation between Supervisory Authorities
Safety Measures	Supervisory Review Process—Quantitative Tools	Supervisory Reporting and Public Disclosure
Solvency Capital Requirement: Standard Formula for Life and Non-Life	Transparency of Supervisory Action	Pro-Cyclicality
Solvency Capital Requirement: Internal Models for Life and Non-Life and Their Validation	Investment Management Rules	Small and Medium-Sized Enterprises
Reinsurance (and Other Risk Mitigation Techniques)	Asset-Liability Management	
	Pillar Two—2nd Wave	
	Quantitative Impact Study and Related Issues	
	Powers of Supervisory Authorities	
	Solvency Control Levels	
	Fit and Proper Criteria	
	Peer Review	
	Group and Cross-Sector Issues	

EXHIBIT 42.4 THREE WAVES OF ADVICE

42.9 CONCLUSION

The insurance industry will undergo a major and profound transformation under Solvency II. The demands for much more robust capital management, internal controls, and financial transparency will stress many organizations. Even large global firms will be challenged in their ability to normalize and standardize many years' worth of internal data. All firms will find qualified internal and external experts in risk management difficult to come by and demanding premiums for their services.

It is logical to predict that banking's experience with Basel II will be repeated in the insurance industry. Compounding the problem, rating agencies will raise the bar ahead of the regulations. This is not a criticism of rating agencies in that they will be hard-pressed to offer the most favorable ratings to organizations not meeting the elevated standards. Once one player hits the mark, others will be expected to follow. The efforts and costs to do this are enormous and will require:

- Streamlined back-, middle-, and front-office software applications
- Robust IT infrastructures using COBIT, ISO 17799, and other best practice frameworks

- Business process resiliencies far beyond disaster recovery programs
- Enterprise-wide content management that includes documents, records, e-mails, and both logical and physical controls
- Clean historical data that is consistent across an enterprise and is normalized over several years' worth of history—a huge task for even the best-run enterprises
- A focused and chartered senior and middle management with the expertise, training, budget, and time to make this happen
- Outside support from experts, who will be in short supply

Smaller and less sophisticated firms will be particularly stressed to meet these higher standards. Solvency II and Basel II will reinforce each other in the marketplace. Increased corporate governance requirements coming to almost all major economies will play a role as well. As a consequence, it is reasonable to expect a major consolidation in both industries. Even if smaller organizations fall below the regulatory requirements of the standards, their costs of doing business will be higher, and possibly much higher than those meeting and exceeding mandates of Solvency II, Basel II, and national corporate governance mandates.

Notes

1. See the IAIS's web site: www.iaisweb.org/.
2. See the IAIS's "A New Framework for Insurance Supervision: Towards a Common Structure and Common Standards for the Assessment of Insurer Solvency," October 2005.
3. IAIS, "A New Framework for Insurance Supervision: Towards a Common Structure and Common Standards for the Assessment of Insurer Solvency," October 2005, 7–8.
4. Ibid., 6–7.
5. IAIS, "The IAIS Common Structure for the Assessment of Insurer Solvency," February 2007.
6. Conning Research and Consulting, press release, May 15, 2006.
7. See the European Commission's Financial Services Action Plan: Progress and Prospects Expert Group on Insurance and Pensions, Final Report, May 2004.
8. European Insurance and Reinsurance Federation (CEA), "Solvency II: Understanding the Process Is Indicated," Brussels, February 2007, 18. www.cea.assur.org.
9. See the Bank for International Settlements, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework" (known as Basel II), June 26, 2004.
10. IAIS, "Issues Paper on Solvency, Solvency Assessments and Actuarial Issues," March 2000.
11. See Directive 2006/48/EC of the European Parliament and of the Council, "Relating to the Taking Up and Pursuit of the Business of Credit Institutions," June 14, 2006.

12. Noël Amenc, Lionel Martellini, Philippe Foulquier, and Samuel Sender, "The Impact of IFRS and Solvency II on Asset-Liability Management and Asset Management in Insurance Companies," November 2006, www.edhec-risk.com/ALM/ifrs_solvency_II/index_html.
13. Wikipedia, "Lamfalussy process," http://en.wikipedia.org/wiki/Lamfalussy_process.
14. See the European Insurance and Reinsurance Federation (CEA), "Solvency II: Understanding the Process Is Indicated," Brussels, February 2007, 5. www.cea.assur.org.
15. KPMG, *Insurance: Solvency II Briefing, Edition Number 1* , November 2006, 4.

CHAPTER 43

ISLAMIC FINANCE

Sabah M. Ali Mahmoud

43.1 INTRODUCTION

(a) GENERAL. In today's world dominated by globalization, technological and communications advances, expanding world trade, and investments, there seems to be a resurgence of the application of basic principles of shariah in Muslim countries, particularly in financial transactions. This trend is also gaining importance

in countries of the western hemisphere where rapidly increasing numbers of Muslims are living or through the expansion of business and investments in or with countries that have an Islamic majority.

The aforementioned trend has led to the increasingly expanding and developing concept of Islamic finance. In the past few years this area of international finance has substantially developed. It is reported that over 70 Islamic banks and investment funds were established, not only in Islamic countries but worldwide as well, that have an estimated amount of approximately $80 billion under management.

Therefore, we believe it is extremely important, in conducting business in or with the Middle East and in countries with a Muslim majority such as Iran, Pakistan, Malaysia, and Indonesia, or in dealing with matters related to the region, to at least be aware of the main principles applicable to Islamic finance, which is becoming an increasingly important topic not only to bankers, financial institutions, and other professional practitioners such as lawyers and accountants, but also to individual businesspeople and government officials as well.

It is important to note that in parallel with the rapid growth of Islamic finance there has been an equally dramatic emergence and growth of ethical finance as a global phenomenon. It can be argued that Islamic principles in finance effectively make it a subsector of ethical finance.

(b) BASIS OF SHARIAH RULES. Prior to dealing with the specific shariah rules that apply to Islamic finance, it will be useful to briefly explain some of the main basic principles of shariah and Islamic jurisprudence.

Shariah is primarily based on the text of the Holy Qur'an. The Qur'an consists of 114 *Suras* and is the manifest revelation communicated to the Prophet Muhammad (*GBPH*)[1] in approximately the year AD 610.[2]

The established practices and teachings of the Prophet (*GMPH*) (*Al Sunnah*) form an important second source of shariah.[3]

Over the centuries, since the advent of Islam, shariah has developed through extensive research and interpretation of Islamic scholars. The consensus of opinion of scholars (*ijma*), defined as the unanimous agreement of Islamic scholars after the demise of the Prophet on any specific matter; analogical interpretation (*qiyas*) defined as an analogy warranted when a solution to a new matter cannot be found in the Qur'an; and the *sunnah*, or a definite *ijma*, form the third sources of shariah.[4]

(c) GENERAL SHARIAH PRINCIPLES. It is important to note that Islam as a religion and shariah not only provides rules of personal behavior but also has numerous verses that deal with and regulate matters related to civil, commercial, and business transactions and dealings (*muamalat*) as will be mentioned later.

However, it is further to be noted that there has not been a uniform application of shariah. Countries in the Middle East, Africa, and the Far East with a

predominantly Muslim population have, to varying degrees, adopted laws based on shariah, which, in spite of similarities, relied on varying interpretations of shariah according to the predominant Islamic sect applied in that specific country. In this regard it is important to realize that there are two main Islamic branches, namely Sunni and Shia, with different interpretations and emphasis of specific shariah rules. The Sunni branch in turn has four main sects, namely, the Hanafi, Shafi, Maliki, and Hanabli sects.

Another important point to be noted is that a current uniform codified text of shariah does not exist. Historically, during the Ottoman rule of most of the Middle East, which continued until the end of World War I, shariah was codified and applied in these countries. *Majalat Al-Ahkam Al-Adlia* (*Al-Majala*), the Civil Code of the Ottoman state, was based on shariah mainly derived from the Hanafi sect applied by the Ottomans, compiled by jurists, and promulgated in Istanbul in the Islamic year 1286 H (i.e., 1836).[5] Even though the application of *majala* was continued for a while in these Arab Middle Eastern countries, after their independence these countries promulgated their own civil codes and no longer applied *Al-Majala*. However, *Al-Majala* is still considered an important reference to shariah rules.

Another important fundamental general principle of shariah provides that for a matter to be forbidden, it has to be specifically prohibited in the Qur'an or *Sunnah*. In other words, it should be specifically forbidden (*haram*). Without such specific prohibition, a matter is considered allowed and lawful (*halal*). This might seem fairly straightforward, but difficulties could occur in the interpretation and application of what is allowed or prohibited.

At the core of Islamic finance is the fact that usury (*riba*), for some interest payment, is forbidden (*haram*). Money in Islam is not allowed to be used to make more money. However, profits (*arbah*) from business are allowed (*halal*). The Qur'an quite clearly specifies that while profit and usury may seem similar, the first (*arbah*) is allowed, but usury is prohibited, as will be further explained in the following section.

The challenge therefore for Islamic finance is to structure transactions in such a way that interest is not involved, while profits and fees are utilized to achieve the required returns. In conjunction with this, there will always be subtle differences in the underlying risks that are part of the product or deal.

43.2 SHARIAH BUSINESS RULES

(a) TRADE. Mecca in the Arabian Peninsula, where the Prophet (*GBPH*) was born, raised, and received the Revelation, was in the pre-Islamic period an important center of trade and commerce. Goods and products were exported and imported, usually in caravans to neighboring countries. The financial resources to arrange for this trade were based on different forms of finance and investment, such as providing funds by a person to another to invest in the purchase of goods for a share of the return (*mudarabah*), partnership (*shirkah*), and even

borrowing money on an interest basis, which was later prohibited, as will be mentioned later.[6]

In fact, the Prophet (*GMPH*) was, for many years, engaged in trade buying and selling goods between Mecca and Syrian cities.

The Qur'an confirms that trade is allowed, stating that "God has permitted sale (trade) and forbidden usury. . . ."[7]

Therefore, shariah rules clearly generally allow trade. Therefore, while trade and investment should only be in things that are allowed and are considered lawful (*halal*), which are permitted under shariah, such trade and investments are neither allowed nor permitted in things considered sinful (*haram*), which broadly include things that might also be prohibited in other countries, such gambling and matters related thereto; drugs, alcohol, or products and goods that are prohibited; as well as other immoral activities such as prostitution or pornography.

(b) CONTRACTS IN SHARIAH. Contracting as a legal concept is specifically provided for in the Qur'an, where it is clearly specified that parties to a contract should fulfill their contractual obligations, stating that "Ye who believe fulfill the contracts. . . ."[8]

A specific verse in the Qur'an further requires that contractual obligations, particularly borrowing, should be transcribed, stating that "Ye who believe when you enter into a debt for a specific period of time, have it written down and let a just scribe transcribe it between you. . . ."[9]

A further general shariah rule that confirms the sanctity of contracts provides that contracts shall be the binding law between the parties. A recognized statement of the Prophet (*GBPH*) provides that Muslims are bound by the contractual obligations.[10]

Al-Majala, as mentioned earlier, is still considered a reference to shariah rules and reiterates this principle by providing in the definition adopted for contracts that "the contract is the pledge of contracting parties in their undertaking a matter and is the joining of an offer with an acceptance."[11]

43.3 USURY (*RIBA*) AND INTEREST

(a) PROHIBITION OF USURY. The term *usury*, translated in Arabic as *riba*, *is* usually defined as charging a fee for the use of money borrowed and is also generally interpreted to mean charging excessive and compounded interest for money lent. During the dawning of civilization in Babylon, a system of credits was developed that was based on the major commodities known at the time that prohibited excessive charges.[12]

Historically, usury was universally condemned as an immoral act. Holy books of all religions have provided for this attitude, particularly since the concept generally symbolizes greed and exploitation of the needs of the borrower.[13] In fact, even in modern Europe usury was, until the mid-nineteenth century, considered illegal in some countries, such as the United Kingdom.[14]

Usury is clearly prohibited in shariah, as there are numerous verses of the Qur'an providing for that prohibition, particularly the verse that states that "those who devour usury will not stand except as stands those whom the devil has touched with madness; they say that trade (sale) is like usury but God has permitted trade and forbidden usury. . . ."[15]

Numerous other verses in the Qur'an reconfirm this prohibition, namely, "Ye who believe, you shall not take (consume) usury, compounded over and over and obey God, that you may succeed."[16]

Other verses further confirm this prohibition by stating, "And for taking usury, which was forbidden to them, and for consuming the people's money illicitly; we have prepared for the disbelievers among them painful retribution" and "And the usury that is taken to increase some people's wealth, does not gain anything with God."[17]

Therefore, while in accordance with the aforementioned verses there can be no doubt or argument that shariah prohibits usury (*Riba*), an argument was made concerning the terms *usury* and *interest*, their definitions, the relationship between the two concepts, and whether all interest is considered usury. This controversial point will be discussed in more detail later.

(b) INTEREST. Interest is generally translated in Arabic as *faidah* and was usually defined as charging a fee for the use of money. Although many Islamic jurists and scholars have argued that all forms of interest charged constitute usury,[18] others have argued that only excessive compounded interest charged at exorbitant rates is usury and that agreed simple uncompounded interest does not constitute usury. It was reported that a scholar at Al-Azhar University (a renowned Islamic university in Cairo, Egypt, and a leading Islamic study and research center), had stated that bank interest was not un-Islamic.[19]

In support of their argument, the latter group who claim that interest is not prohibited refer to the aforementioned shariah concept of "the sanctity of contracts" and further argue that the Qur'anic verse, again mentioned earlier, states that "you shall not take (consume) usury, compounded over and over." They consider this to limit the prohibition to compounded interest charged time and again only, and does not include or apply to duly concluded contracts for financial facilities providing for simple interest that they argue will be legally valid between the parties.

This controversial interpretation of usury created an important practical precedent in the Gulf when in the early 1980s the United Arab Emirates (UAE) Federal Supreme Court (colloquially referred to as the Court of Cassation) decided to adopt the strict interpretation of shariah rules that all interest is considered usury.[20]

That decision created havoc in the courts and for the banking system in a country that applies a liberal free-market economy with a thriving banking structure, particularly in Dubai, one of the main Emirates that formed the UAE.

In Dubai the courts that operate outside the jurisdiction of the Federal UAE judicial system refused to endorse this decision of the Court of Cassation and continued to uphold contracts and agreements concluded between banks and their clients for overdraft and other banking facilities.

However, elsewhere in the other Emirates numerous cases were initiated in the courts claiming the reimbursement of interest charged and paid. Consequently, the UAE Central Bank, which itself normally charges banks interest rates on a commercial basis, had to issue a directive on the method of calculating interest.[21] This controversy continued until a compromise position was reached to allow simple noncompounded interest with 12 percent as the maximum rate to be charged and deducted every three months.

43.4 ISLAMIC FINANCE

(a) DEVELOPMENT AND EXPECTATIONS. Although, as mentioned earlier, there had previously been different forms of trade finance in the Islamic region, the first modern Islamic banking venture is reported to have been embarked on in Egypt over 40 years ago as an undercover savings bank based on profit sharing.[22] This innovative banking system rapidly expanded to other countries and developed during a comparatively short period to become a recognizable financial business, mainly concentrated in the Gulf region, the Middle East, and North Africa, as well as Iran and Malaysia.

Obviously, the worldwide increases in oil prices has led to substantial increases of oil revenue to oil-producing countries in the Middle East, which have a predominantly Muslim population. This increased revenue created a natural cycle that led to increased public spending that in turn led to the flow of assets to both the public (governmental) and private sectors. Public sector investment organizations, including entities owned by governments such as public investment authorities, companies, and businesses, benefited from this flow of revenue as well as private sector companies and individuals. Consequently this cycle led to a significant improvement of the cash flow in these countries and the availability of investment funds. It can be reasonably anticipated that a portion of this increased investment potential will ultimately flow to Islamic banks and Islamic investment funds.

The banking system established in most of the countries in the Middle East is based on globally applied Western banking policies and procedures. The general banking sector in the Arab Middle East is reported to have about 470 Arab banks managing assets that are worth more than US$1 trillion, US$632 billion of which is deposit-based. It was further reported that in spite of the fairly steady growth of the banking and investments sector in the Middle East, banks and investment funds in the area are reported to be looking for expansion beyond the Middle East, with the Far East, Asia, and Europe providing potential investment opportunities.

The general application of Western conventional banking policies did not prevent quite a few banks in the area from either operating on Islamic finance principles or establishing divisions that operate on an Islamic basis.

Although we do not believe accurate statistics have been published on the volume of Islamic finance, it had been reported that assets controlled by Islamic banks globally are estimated at between $200 billion and $500 billion, with an estimated growth at the rate of 10 to 15 percent per annum.[23]

This new trend of the application of Islamic finance is not limited to countries in the Arab Middle East and North Africa, but also extends to countries with a predominantly Muslim population, which have in fact made significant progress in applying an Islamic-based economy including Islamic finance, such as Iran, Pakistan, and Malaysia.

However, in spite of its expansion, Islamic finance still represents a small portion of the global banking system, and general skepticisms still remains in some financial quarters concerning the application of Islamic finance concepts and principles.

But, in the past few years there has been a notable overall change in the attitude in financial centers toward this expanding banking and investment system, coupled with keen interest in learning how it operates. This interest is enhanced not only by the possible flow of available funds mentioned earlier but also by the global increase of the number of Muslims living in the western hemisphere. It is reported that there are 1.8 million Muslims living in the UK only, with an additional half million regular visitors, and approximately 12 million Muslims in the European Union, particularly in France and Germany.[24] There are also substantial Muslim communities in other European countries, estimated to be over 50 million, as well as those in countries of the western hemisphere such as the United States and South American countries.

Consequently, in recent years the UK Financial Services Authority (FSA) has allowed banks to provide Islamic financial products in the internationally important London financial market to be offered from a number of High Street banks that offer current accounts and mortgages tailored for Muslims. The FSA has also reported that the UK is the home of the first shariah-compliant retail bank in the West, the Islamic Bank of Britain, authorized to operate in 2004. The European Islamic Investment Bank was also authorized to operate as the first investment bank.

(b) GENERAL PRINCIPLES. Unlike conventional Western-style banking that is generally based on charging or paying interest on deposits, borrowing, and for providing facilities, the predominant overriding principle of Islamic finance is that it should be interest free and based on the concept that the banks and their clients are partners in investment or trade that are performed by the Islamic bank using deposited funds.[25]

Even though Islamic banks, similar to conventional banks, are profit oriented, they are also supposed to be compassionate as well as be aware of and uphold the overall welfare of the community where they operate, as will be mentioned in more detail later. One of the practical applications of this principle is that banks should comply with a verse in the Qur'an that states that a person in need such as a debtor who owes the bank money should be given leeway until he can improve his situation.[26]

Another important general basic principle of Islamic finance is that funds should be invested in matters that are allowed and lawful (*halal*) and not in anything that is forbidden (*haram*) in accordance with shariah principles, as explained earlier in the paragraph on general trade in shariah.

Therefore, Islamic investment, similar to trade, should conform to shariah rules, and should not be used in matters that are prohibited or considered immoral in accordance with shariah. It is also important to note that although trading in goods and products is allowed, the selling of debts and the generation of money from the use of money is prohibited in shariah. Other prohibited matters that were mentioned earlier include any that involve gambling, drugs, alcohol, products and goods that are not allowed, and immoral matters such as prostitution or pornography.

Banks operating on Islamic principles are required to establish and appoint advisory boards, committees, or consultants that are considered shariah experts to advise the bank by reviewing investment policies and assisting the management in making decisions concerning specific business prospects to avoid any controversial businesses and ensure that the operations and activities of the bank comply with shariah principles.

(c) INVESTMENT PRODUCTS. Even though Islamic banks and finance usually have an overall traditional community welfare aspect to their operations, they have, similar to conventional Western banks, the ultimate objective of creating profits for their shareholders and depositors through specific Shariah-compatible investment devices or products. However, as mentioned earlier, the overriding principle of Islamic finance is that it should be interest free and its investment instruments should conform to and be in accordance with shariah. The main Islamic finance products/devices are listed next.

(i) Deposits (Wadiah). Deposits are usually defined as a sum of money paid by a customer/depositor for a specific period to a bank to be repaid to the customer on agreed terms.[27] In both conventional and Islamic finance, deposits usually form the main source of investment revenue. However, the difference between the two methods of banking is that while in conventional banking the repayment of the deposit is guaranteed by the banks, in Islamic banking the bank is considered the keeper and trustee of funds to be invested on the basis of partnership between the depositor and the keeper; consequently, the bank does not guarantee the repayment of deposits.

Deposits invested by Islamic banks in accordance with shariah could obviously generate profits as well as incur losses. Therefore, the bank will not guarantee deposits. This concept created conflict in some jurisdictions such as the UK where the law requires the bank to safeguard the deposited funds. This conflict was resolved by requiring the Islamic bank to conform to the law and offer full repayment of the deposits but inform the depositor of the risk-sharing formula and allow the depositor to either accept or refuse full payment in accordance with his religious convictions.[28]

As for the payment of interest on deposits, here again differences occur between the two methods of banking. In conventional banking depositors are paid interest calculated as a percentage of amounts deposited, but in Islamic finance interest is not paid. However, in some cases Islamic banks have devised an alternative method, whereby they will not pay interest but may reward the depositor with a gift (*hibah*), which, as a gift, is unilaterally decided and not guaranteed.[29]

(ii) Investment Finance (Mudarabah). Investment finance (*mudarabah*) is, as mentioned earlier, one of the oldest forms of Islamic investment and finance whereby the capital owner/financier/ Islamic bank agrees to provide specific investment funds to an entrepreneur (*mudarib*) to be invested as he deems fit using his skills and expertise. Although the bank will not participate in the management of the businesses financed, it would usually supervise it to ensure that funds are invested in accordance with the agreed terms.[30] Traditionally, this form of finance generally involved providing finance for the purchase and sale of goods and products for a share of the return. In providing this type of investment finance, the Islamic bank will be considered both as capital owner/financier to the entrepreneur, while at the same time the bank itself is an entrepreneur that manages deposited funds of the depositors. This is usually described as two-tier investment (*mudahrabah*).[31]

An important condition of this type of investment is that while both parties share in profits as agreed, only the capital owner or provider will bear the losses incurred unless such loss is caused by the misconduct or negligence of the entrepreneur (*mudarib*). The investment finance will continue until the finance is repaid. In this investment the bank will consider itself as compensated for the time value of its money in the form of a floating rate that is calculated on the basis of profits made.

(iii) Partnership (Musharakah). Partnerships or joint ventures (*musharakah*) are again traditionally one of the oldest forms of Islamic finance whereby a partnership is concluded between the financier who will mainly provide the finance and another party or parties to perform a specific business venture that will include the management arrangements of the venture and its supervision. Profits made and losses incurred usually will be divided and shared on an agreed ratio based on the equity participation. Providing qualified management personnel by Islamic banks for the venture could pose a difficulty for the banks, which, bearing this difficulty

in mind, would be more generally inclined to invest funds in stocks and shares of public or private companies rather than enter into business partnership ventures.

(iv) Resale Contracts (Murabahah). This Islamic investment concept is essentially considered a resale contract for the purchase of generally durable goods and possibly real estate identified by the buyer or business person to be financed and purchased by the bank in its own name to be resold to the buyer on an agreed immediate or deferred payment arrangement, which will include a profit margin agreed by the parties. The purchase and sale price, other costs, and the profit margin must be clearly stated at the time of the sale agreement. This type of finance is considered to comply with shariah since it is a resale of an asset by the bank that takes title of the asset to resell it.

While the mechanism for calculating the agreed resale price could in fact be on the basis of time value of money similar to calculating interest on a loan, the asset will remain the property of the bank until full repayment of the agreed sale price. However, the bank should not charge interest on late payments. These types of *murabahah* transactions might be considered similar to hire-purchase or rent-to-own arrangements for assets in some jurisdictions.

(v) Lease to Own (Ijarah). The Arabic word *ijarah*, translated as rent, usually indicates the transfer of the right of use of an asset or property by the owner to another party for an agreed term and price. In essence it is fairly similar to the lease or rent-to-own arrangements referred to earlier and is more generally used for real estate purchase whereby the intended buyer will identify the property to be purchased and agree on a price with the vendor; the financier/bank will purchase the property in its name and lease it to the buyer for a specified periodic rental amount for an agreed period. At the end of that period and the payment of the installments the title will be transferred to the buyer as agreed.

This concept is similar to a conventional mortgage but with the difference that funds are not borrowed for an interest to purchase a property, but the bank will share with the ultimate buyer the purchase of the property at the agreed price. The buyer will pay rent on the share of the bank in the property, and can also purchase the property earlier.[32]

(vi) Fabrication Finance (Istisna'a). *Istisna'a* can be translated as fabrication or industrialization. This indicates that this type of product is essentially a contractual agreement whereby cash payments are advanced to finance the fabrication of goods and commodities for delivery at a later date to be sold and to repay the advanced payments. This product is also used for providing the financing for construction of houses, buildings, plants, industrial projects, and construction assets. The contracting parties will agree the specifications of the house or building to be constructed either on land owned by a customer or to be purchased, as well as the construction costs and repayment terms thereof.

(vii) Bonds (Sukuk). *Sukuk*, which could be translated as documents or even checks, is a new and expanding innovation in Islamic finance and designates a financial debt product that is similar to conventional banking bonds. However, in view of the aforementioned fundamental shariah principle that Islamic banking and finance should be interest free, the issuance of tradable fixed-interest-bearing bonds is not permissible in shariah. Therefore, the issue of *sukuk* should be on the basis of investment products that are allowed and acceptable in shariah, and the funds raised should be used to generate revenue from shariah-compliant assets and products. A good analogy for the type of business for *sukuk* to be invested in might be ethical or green investments. Numerous innovations are being introduced into the growing *Sukuk* market, such as contracts described as *Bai Al-Arboon*, translated as down payment sales, which are similar to options. *Tasaheel* and *Tawreeq* are further new Islamic products being introduced.

Malaysia has been quite active in the *sukuk* market and has recently announced the issue of $750 million worth of tradable Islamic bonds by the Malaysian Government Investment Company (National Khazna).

(viii) Islamic Equity Funds. Trading in stocks, shares, and similar equities is allowed in shariah, and it is usually done through Islamic equity funds that will, similar to *Sukuk* mentioned earlier, invest in shariah-compatible equities.

The Islamic investment equity funds market is again one of the growing sectors within the Islamic financial system. It has been reported that there are currently about 100 Islamic equity funds worldwide that manage total assets of approximately US$1 billion and the market is growing by 12 to 15 percent per annum. In spite of skepticism about the performance of some of these funds (some of which had to close down), it is still expected that the continued interest in Islamic finance will lead to more similar Islamic equity funds being launched, probably by some major Western banks and financial institutions.[33]

(ix) Benevolent Loans (Qard Hassan). This kind of loan is generally considered as a contribution of Islamic banks to community welfare and is extended for benevolent and charitable reasons whereby a loan is given by the bank to a person in need, who will only be required to repay the actual amount borrowed. Occasionally, while the borrower is obliged to repay only the amount borrowed, there might be a discretionary extra amount paid by the borrower to cover possibly banking or administrative costs. This product is a genuine interest-free loan that some will consider as the only type of loan that does not violate the prohibition on usury or interest, since it is a loan that does not compensate the creditor for the time value of money.

(x) Sales Contracts (Bay'). As mentioned earlier, trade that is the general exchange of goods, products, or property is allowed in shariah and is customarily concluded through either barter arrangements or sales contracts.

While shariah recognizes different types of sales, depending on the transactions concluded, it prohibits others. In addition to *murabaha* and other contracts mentioned earlier that involve sales contracts as well, Islamic banks could finance certain types of sales contracts for customers. These could be contracts for the sale of goods at an agreed lump-sum price to be paid at a later date or by payment of installments (*bay' mu'ajjal*). The bank would buy the goods on behalf of the customer and then sell them to him with an agreed markup to be paid for later. This type of sale is similar to conventional deferred payment sales without the need to specify the bank's profits. Another type of controversial sale contract is to make an advance payment for the purchase of goods to be delivered at a later date (*bay' salam*). This is similar to forward buying. However, it should be for defined goods to be delivered at a specific date and should not include gold or silver, which are usually equated to money so that trade therein is not acceptable in shariah.

Another type of unacceptable sale is called *bay' al gharar*, which is usually described and translated as a sale that includes an unknown or deceptive element. In shariah contracts that could involve deception of a contracting party or uncertainty about whether the essential elements of a contract are prohibited. *Gharar* contracts are typical of contacts whereby sales of an unknown or unspecified matter are not allowed. Gambling is a typical form of prohibited *gharar*.

(xi) Joint Liability (Takaful). While insurance has become an essential factor in modern conventional business to reduce risks, it is neither recognized nor allowed in shariah, mainly because it involves an element of uncertainty and ambiguity, described earlier as *gharar*. However, the concept of *takaful*, which signifies joint responsibility or cooperation, has been accepted since the advent of Islam. This concept is similar to mutual insurance whereby members share losses of assets or properties of other members.[34]

43.5 JORDAN ISLAMIC BANK FOR FINANCE AND INVESTMENT

(a) BACKGROUND AND INCORPORATION. This part of the chapter provides a practical case study concerning the incorporation and operations of the Jordan Islamic Bank for Finance and Investment that relies on research of the bank documents, the paper prepared by a senior officer of the bank, as well as meetings with the bank officials.[35]

The Royal Hashimite Kingdom of Jordan issued the Banks Law No. 24 of 1971, later replaced by the Banks Law No. 28 of 2000 (the Banking Law), which is the currently valid and applied law that regulates banking operations in Jordan, including Islamic banking.

Paragraph A of Article 2 of the Banking Law defines an Islamic bank as "the company that is licensed to perform banking business in accordance with rules of Islamic *Shariah* and its principles as well as any other business and activities in accordance with the provisions of this law." The same article further

defines Islamic banking business as "the business established on non-interest basis in the area of accepting deposits and other banking services as well as in the field of finance and investment in accordance with the rules and principles of Islamic *Shariah*."

In addition to its general provisions, the Banking Law also provides specific detailed Articles 50 through 58 that apply to Islamic banks. These articles highlight the interest-free aspect of Islamic banking. The objectives of an Islamic bank are listed as providing banking services and performing finance and investment business on a non-interest basis whether in accepting or giving all forms and types of such services; to develop ways of attracting funds and savings and to direct them to participate in investment banking established on non-interest basis; to provide services that will create forms of organized joint social cooperation on mutually beneficial basis.[36] In Article 52, the Banking Law provides the detailed types of banking business that Islamic banks are allowed perform that include the accepting of deposits, issuance of certificates and bonds, and performing a variety of extensive interest-free financing and investments that will be acceptable to the Jordan Central Bank.

In accordance with the provisions of the Banking Law, Islamic banks also have to undertake to implement the rules and principles of shariah and should, in accordance with their memoranda and articles of association, appoint a "*Shariah* supervisory commission" of at least three persons to supervise the activities of the bank, ascertain that these activities are compatible with shariah, provide advice concerning contracts, and perform any other matters that are required by the Jordan Central Bank.[37]

The Jordan Islamic Bank was initially established in accordance with Temporary Law No. 13 of 1978, later replaced by Law No. 62 of 1985, which in turn was revoked when the Banking Law was issued. The bank was incorporated as a public joint stock company duly registered in accordance with the Jordan Company Law in 1978 adopting its Memorandum and Articles of Association.

In accordance with the law incorporating the bank, its initial capital was listed as 4 million Jordanian dinars (JD),[38] later increased in accordance with provisions of its Memorandum and Articles of Association to reach 40 million JD. It is reported that the bank has now expanded to become the third largest bank in Jordan. Its 27th Annual Report of 2005 reported a total bank budget of 1.32 billion JD, representing an increase of nearly 18 percent. This figure will increase to 1.55 billion JD if the balances of the registered investment accounts and investment portfolios are added. The bank's pretax profits were reported to have reached over 20 million JD.

(b) IDEOLOGICAL CONCEPTS AND OBJECTIVES. The Jordan Islamic Bank, in addition to observing the provisions of the Banking Law that stress the importance of shariah, as an Islamic bank has to uphold and maintain ideological concepts and methods of operation compatible with shariah. As emphasized earlier, the

main overriding principle of Islamic banking is that it should be interest free and not based on the conventional banking concept of borrowing or lending operations and should provide finance and invest available funds in shariah-allowed business. Islamic banks should, in addition to being investment entities, also have a wider development and social role that not only will cover the management and supervision, when designated, of welfare funds and charitable societies where religious contributions (*zakat*) are paid, but also should encourage the establishment of an Islamic economic system that will achieve overall economic, financial, and social development in the communities where they operate.

Therefore, in spite of the Islamic bank upholding shariah fundamental principles and general welfare and humanitarian precepts, business operations will obviously have to be profitable. In other words, business operations should not only be investment oriented but also aim at achieving overall community development and social cooperation.

Furthermore, a practical ideological concept of Islamic finance becomes apparent concerning the treatment of banking debts. In conventional banking, defaulting debtors are mainly dealt with in accordance with agreed terms and conditions that usually include the application of additional charges and penalties without much consideration given to personal difficulties. However, in Islamic banking defaulting debtors have to be dealt with more compassionately and with consideration of personal situations. In this regard an Islamic bank should uphold the previously mentioned overriding principles that banking operations should be interest free as well as comply with the verse in the Qur'an that provides that a person in need should be given leeway until he can improve his situation. The application of granting this latitude requires that the bank should not charge any additional fees on delayed payments. In spite of this, banks sometimes take the view that this does not prohibit a bank from charging a penalty in the case of a financially able but defaulting customer in application of the religious edict (*fatwa*) made in this regard in compliance with the statement of the Prophet (*GBPH*) that "the procrastination of the rich is unjust."[39]

The bank's Memorandum and Articles of Association provide its wide objectives that generally have to be compatible with the provisions of the aforementioned mandatory Banking Law that reiterates that an Islamic bank's objectives and operations have to be free of usury (*riba*). These include providing a wide range of banking, finance, and investment services to cover economic and social requirements. The objectives particularly refer to the expansion of banking transactions by providing usury-free services; promoting means of attracting funds and investments to be invested in usury-free banking methods; and providing necessary finance for the needs of the different sectors, particularly those that are not interest-related banking facilities.

To achieve its objectives, the bank could perform the businesses listed under three headings, namely, "usury-free banking business," "social services and finance," and "investment services." Under each heading there is a fairly

comprehensive detailed list of items that the bank can perform, which include accepting deposits, opening current and deposit accounts, paying and endorsing checks drawn, collecting commercial papers, transferring funds, opening documentary credits, issuing banking and letters of guarantee, issuing credit cards, and all other banking services.

Further detailed services that the bank could perform allow it to deal in foreign currencies, provide interest-free loans, manage assets, provide advice and research to customers, establish and manage social funds, and provide finance on *mudarabah*, diminishing partnerships, and *murabaha* basis as well as invest available funds in different projects.

In accordance with the provisions of the Banking Law referred to earlier, the bank has appointed a four-member shariah supervisory commission that will present its reports to the Annual General Assembly confirming that the bank's operations and activities were compatible with shariah.

(c) INVESTMENT FUNCTIONS AND PRODUCTS. This part of the chapter provides a brief idea of the Jordan Islamic Bank's main financial and investment activities and products, which are similar to the Islamic investment products referred to earlier. In the final analysis it is essential to note that the implementation mechanism of the products has to conform to shariah principles.

(i) Deposits. As mentioned earlier, deposits, in both conventional and Islamic banking, constitute the main source of banks' investment funds. However, again as mentioned earlier, there are fundamental differences in the treatment of deposits in these two systems of banking. In conventional banking, deposits take the form of loans whereby the depositors will, in accordance with the deposit arrangements, practically lend the bank a specific amount of money for a defined period of time at a specified interest rate to be paid on maturity regardless of the business results of the bank. In Islamic banks, the relationship between the bank and depositors is not based on lending or borrowing but is rather on the basis that such deposits are received by the bank as investment funds (*mudarabah*) to be invested, with both sides sharing the results of the investment, benefiting from the gains made or bearing the loss incurred.

The bank mainly provides three types of deposit accounts. The first is the current account, called in some Islamic banks a "trust account," which the bank will hold in trust for depositors and will undertake to honor withdrawals from there or make on-demand repayments of the deposits. Usually the bank will, at its own risk and for its own benefit, invest part of these funds. That means the depositor will agree to forfeit any benefits in return for the bank's safekeeping and guarantee of the deposit.

The second type of deposits is the savings accounts, generally called "joint investment accounts." These accounts will be invested with other bank funds and be subject to profit and loss as an investment (*mudarabah*). There are usually

three types of such deposits depending on liquidity, namely savings, notice, and deferred-deposit accounts.

The third type of account is called the "special investment account" whereby depositors will authorize the bank to invest the funds on their behalf in a specific project or sector for a share of the profits or accept the loss incurred. In return the bank will only be entitled to a percentage of the profit if and when achieved.

In addition, the bank can, in accordance with the provisions of the Banking Law, issue joint or specialized lending certificates/bonds (*mudarabah*) that are usually issued by the bank to whoever wishes to participate in a specific investment deal organized and managed by the bank in accordance with specified terms and conditions, including the type, exchangeability, description of the project, and duration of the investment. The accumulated funds will be invested in the prescribed project in accordance with an investment (*mudarabah*) contract whereby the profits are paid according to the specified ratio, and losses will be borne by only the investors while the bank will lose only the effort it had made unless there is malice or negligence on its part.

(ii) Profit and Loss Sharing Certificates (Quradh/Mudharabah). Paragraph 52(b) of the Banking Law provides that Islamic banks may issue joint or special profit and loss sharing (*muquaradha)* certificates and establish investment portfolios or funds. The bank issues *quradh* or *mudharabah* certificates similar to bonds or *sukuk*, referred to earlier, to customers who wish to join a specific investment operation that the bank organizes and manages according to specific conditions designating the category of the certificate, transferability, details of the project, and duration of the investment. Accumulated funds of these certificates are invested in the specific projects with profits disbursed according to agreed percentages and the loss will be borne only by the investor (*mudharib*); here again the bank will lose only its time and efforts.

The bank also provides investment finance on a *mudharabaha* basis whereby it will finance a specific venture with one or more customers providing time and effort and sharing profits, with capital loss being borne by the bank and the investors losing only their time and efforts.

(iii) Joint Ventures (Musharakah). This type of product represents the Islamic bank's participation in projects that could be either a fixed joint venture (*musharakah*) or a receding venture that will end in ownership. The first (fixed) venture is a straightforward partnership whereby the partners will share for the duration of the venture or company until it is terminated or liquidated and proportionately share the profits and losses. The second (receding) venture represents participation by the bank whereby it will participate in the finance of a specific project and share the net profits except for a designated portion thereof that will be paid to reimburse the original capital finance, and once this is reimbursed it will be owned by the customer.

(iv) Sales (Bay'ou). As mentioned earlier, trade is in principle an allowed vocation accepted and practiced in shariah, which should be in goods that are allowed and not prohibited. Consequently Islamic banks can and usually do invest directly in trading functions by entering into sale of goods and products (*bay'ou*) contracts or indirectly providing finance to their customers for such sales. There are different types of sales contracts that are mainly considered as shariah-compatible. One of these is the deferred payment sale (*bay' aajil*) whereby the bank will agree to purchase the goods to be sold for a price with a specific profit margin to be paid for either in cash or in installments, provided that the two sales are not concluded at the same time. Another type of sale represents a reversed payment contract called *bay' salam* in which the parties agree on the sale price prior to the goods being ready for delivery, such as the sale of agricultural produce before it ripens. Then there is the contract for the sale of goods such as commodities on *murabaha* on order of a customer who will undertake to repurchase the goods. A further type of sale is the purchase of goods identified by the customer for a price to be determined later with a profit margin and an option for the annulment of the contract that is described as conditional *musawama*.

(v) Fabrication Finance (Istisna'a). This product, mentioned earlier, essentially designates a contractual agreement whereby cash is advanced by the bank to finance the fabrication of goods to be delivered at a later date, the delivery of commodities, and turnkey project finance. The assets involved will be sold to repay the advanced payments. This product can also used to provide financing for construction projects such as houses, buildings, plants, industrial projects, and similar assets.

(vi) Lease to Own (Ijarah). Lease to own (*ijarah*) is a product, again referred to earlier, whereby the bank will, assumably at the request of the customer, purchase different types of assets including machinery and property and transfer the right of use to the customer on lease for a specific period with the ultimate transfer of ownership to the customer when the payments are completed.

This product is being advertised by the Jordan Islamic Bank and marketed to include means of transport such as airplanes and different vehicles, machinery, equipment, and real estate. Parts of important residential developments have also apparently been marketed using this type of product.

(vii) Foreign Investments. To diversify its investment portfolios, the bank is reported to also participate in foreign markets by establishing companies or acquiring shares in other Islamic banks and companies whose business conforms with shariah principles. These foreign markets investments also include making deposits with Islamic banks, funds, and similar financial institutions, as well as entering into external *murabaha* trading deals in commodities and precious metals.

(d) COMMERCIAL PAPERS. In conventional banking, commercial papers such as bank guarantees and letters of credit represent a main part of business activities. Although such papers have become an essential element in global trade, Islamic banks have to deal with these functions in accordance with shariah.

(i) Bank Guarantees. In conventional banking, bank guarantees are usually defined as a written undertaking by the bank that it will guarantee that a customer, with regard to a specified amount of money, will within a specified period perform a specific obligation vis-à-vis a third party. The bank will pay the said amount, usually on first demand, if the customer fails to perform that obligation to the third party, regardless of the objections of the customer.[40] The bank will usually require collateral to cover the guaranteed amount and charge a commission/fee to issue the guarantee and to extend or amend its terms.

In Islamic banking the issue of bank guarantees is a controversial subject. Issuance of a guarantee by a bank for a fee devoid of further services or efforts is not considered acceptable in shariah. However, the issuance of the guarantee would be considered shariah-compatible when the bank enters into some form of joint venture partnership (*musharakah*) with the customer in the business that requires the issue of the guarantee. The argument of this acceptance is based on the theory that the issue of the guarantee was a pledge (*kafalah*) contract that is acceptable in shariah.

The Jordan Islamic Bank's Memorandum and Articles[41] provide that it is allowed to issue bank letters of guarantee. However, the mechanism of issuing the guarantees is not specified. It has been further reported that the bank could issue guarantees for a services fee or commission.

(ii) Letters of Credit. Letters of credit (LCs) that are issued in conventional banking have become the fundamental means of payment in foreign trade transactions and are usually defined as an undertaking of the bank opening the LC issued in accordance with its customers instructions to the beneficiary to pay, accept, or discount the value of notes with the shipping documents when they conform to the specified conditions.

Usually in conventional banking there are two methods of financing the payment of the LC. The first, which is rarely used, is when a customer provides funds to cover the value of the goods to enable the bank to open the LC. The second is when the bank will provide financing to cover the LC for a collateral and charge fees. In Islamic banking while the first method could be acceptable and the bank will charge a services fee for its efforts, the second method will raise problems, namely that the bank will provide finance for a fee. Islamic banks have resolved this difficulty by reversing the arrangement whereby the bank will become totally or partially the owner of the goods and the customer a partner in the transaction.

(iii) Discounting Commercial Papers. The conventional banking practice of discounting commercial papers such as promissory notes is not acceptable in

Islamic banking as it represents the granting of loans for a fee. Here again, when possible, an Islamic bank might consider a form of partnership with the customer to conform to shariah.

43.6 CONCLUSIONS

As mentioned earlier, Islamic finance, in spite of its growth and expansion, still represents a small portion of the global banking system, and general skepticism still remains in financial quarters concerning the application of Islamic banking concepts and principles.

It is important to note that while Islamic finance concepts are fairly simple and straightforward, the application mechanism could be problematic when making arrangements whereby a bank will essentially become its customer's partner.

In certain areas, the practices of some Islamic banks have been opposed because, it is argued, in fact the banks do charge and deal in interest and apply conventional banking methods but provide the necessary legal cover by giving the product or transaction a shariah description while in fact the application mechanism is the same as conventional banking products, or alternatively by giving interest other names or descriptions, such administrative costs or charges.

Therefore, we believe that Islamic finance still has a long way to go to develop in an environment dominated by set conventional banking rules and regulations.

Notes

1. "*Sala Allah Alihey wa Salam*"—God Bless and Praise Him (*GBPH*).
2. See Mohammed Hashim Kamali, *Principles of Islamic Jurisprudence*, the Islamic Texts Society, Cambridge: 1991. 14.
3. Ibid., 44–58. See also Abdur Rahman I. Doi, *Shari'ah the Islamic Law*, 6, 7.
4. Kamali, 168, 197; Doi, 6, 7.
5. Ali Hyder, Durer Al Ahkam: An Interpretation of Majalat Al Ahkam Al Adlia. Al Nahdha Books, Beirut-Baghdad in 1940's.
6. See M. Umer Chapra, *Towards a Just Monetary System*, Islamic Foundation, London 1985. 76.
7. *Al-Baqarah, Sura* II, Verse 275.
8. *Al-Maaida, Sura* V, Verse 1.
9. *Al-Baqarah, Sura* II, Verse 282.
10. "Moslems are bound by their covenants except a covenant that allows a prohibited matter or prohibits an allowed one."
11. Majalat Al-Ahkam Al-Adlia (Al-Majala), the Civil Code of the Ottoman State Article 103.
12. See Hammurabi Code of Laws, http://www.phillipmartin.info/hammurabi/hammurabi_codeindex.htm
13. See Exodus 22:25; Leviticus 25:35, 25:36, and 25:37; Deuteronomy 23:19; Psalms 15:5; Proverbs 28:8; and Jeremiah 15:10.

14. Acts of Parliament known as Usury Laws were repealed in 1854.
15. *Al-Baqarah, Sura* II, Verse 275.
16. *Al-'Imran, Sura* III, Verse 130.
17. Also *Al-Nisa, Sura* IV, Verse 161 and *Ar-Rum, Sura* XXX, Verse 39.
18. The Second Islamic Conference—Cairo, 1965.
19. See "Islamic Banking, Opposition," Wikipedia.
20. UAE Court of Cassation Decision No. 14 of Judicial Year 9, published July 1981.
21. The United Arab Emirates (UAE) Central Bank Directive on interest dated 4/6/1981. http://www.centralbank.ae/law.php.
22. See "History of Modern Islamic Banking," Wikipedia.
23. See Financial Services Authority (FSA) web site, Islamic Banking in the UK. http://www.fsa.gov.uk/.
24. Ibid.
25. See Muhammed Anwar, *Modelling Interest-Free Economy*, the International Institute of Islamic Thought, 1987. 8.
26. *Al-Baqarah, Sura* II, Verse 280.
27. See FSA web site, Islamic Banking in the UK. http://www.fsa.gov.uk/.
28. Ibid.
29. See "History of Modern Islamic Banking," Wikipedia.
30. See M. Umer Chapra, *Towards a Just Monetary System*, the Islamic Foundation, London 1985. 165.
31. Ibid.
32. See Islamic Bank of Britain web site. http://www.islamic-bank.com/islamicbanklive/GuestHome/1/Home/1/Home.jsp.
33. See *Sukuk* in Wikipedia.
33. See "Islamic Banking," Wikipedia.
34. See Institute of Islamic Banking and Insurance web site, http://www.islamic-banking.com/index.php.
35. Baker Al Rayhan, The Theoretical and Practical Basis of Operations of Islamic Banking: The Study, The Islamic Bank of Jordan, 2000.
36. The Jordian Banking Law, Article 50, The Official Gazette of Jordan, 2000.
37. The Jordian Banking Law, Article 58. The Official Gazette of Jordan, 2000.
38. Approximately 0.700 JD = 1 $US.
39. Rayhan, Baker Al, "The theoretical and practical basis of operations of Islamic banking," study prepared for the Islamic Bank of Jordan, 2000, 9.
40. Dr. Abdul Hamid Al Bay'li, *Investments and Shariah Supervision in Islamic Banking and Financial Institutions*, Wahba Books, Egypt, 1991, 47.
41. Subparagraph 1 of Paragraph A of Article 3 of the Memorandum and Subparagraph 1, A, 2 of Article 3 of the Articles.

References

Book of Exodus.

Book of Leviticus.

Book of Deuteronomy.

Book of Psalms.

Book of Proverbs.

Book of Jeremiah.

Durer Al Ahkam, An interpretation of Majalat Al Ahkam Al Adlia, by Ali Hyder Published Al Nahdha Books, Beirut-Baghdad in 1940's.

Financial Services Authority (FSA) web site.

Institute of Islamic Banking and Insurance web site.

Investments and Shariah Supervision in Islamic Banking and Financial Institutions, Dr. Abdul Hamid Al Bay'li published by Wahba Books, Egypt, 1991.

Islamic Banking, Opposition, Wikipedia the Free Internet Encyclopedia.

Modelling Interest-Free Economy, Muhammed Anwar, published by the International Institute of Islamic Thought, 1987.

Principles of Islamic Jurisprudence by Mohammed Hashim Kamali, published by the Islamic Texts Society, Cambridge: 1991.

Shari'ah the Islamic Law, Abdur Rahman I. Doi, published by Ta Ha Publishers, London: 1984.

The Holy Qur'an.

The Jordan Banking Law of published in the Official Gazette, 2000.

The theoretical and practical basis of operations of Islamic banking by Baker Al Rayhan, study prepared for the Islamic Bank of Jordan, 2000.

The UAE Central Bank Directive on interest dated 4/6/1981 published in the Official Gazette.

Towards a Just Monetary System by M. Umer Chapra, published by the Islamic Foundation, London 1985.

UAE Court of Cassation Decision No. 14 of Judicial Year 9 published July 1981.

PART 8

REGIONAL AND NATIONAL GUIDANCE

CHAPTER 44

CORPORATE GOVERNANCE AND RISK MANAGEMENT IN AFRICA

Jackie Young

South Africa has been called the "Hub of Africa" because so many financial and business transactions flow through the country from the rest of the continent. The major South African banks have developed a vast outreach, and now provide services to many other countries in Africa and elsewhere. However, at the same time it is important to demonstrate a solid commitment to good corporate governance practices. Essentially, this entails that South African banks should think how they must approach and attain a reputable and beneficial framework of corporate governance that is aligned with the basic guidelines and requirements thereof. This includes a sound approach to risk management.

This chapter aims to discuss basic concepts of corporate governance and risk management within the African environment with specific reference to the South African banking industry.

44.1 INTRODUCTION

Corporate governance as well as operational risk management are fairly new disciplines that only recently emerged as disciplines in their own right, with many countries, including South Africa, giving them a rightful place as a critical determinant in an organization's management structure.

All the countries on the African continent are regarded as developing countries, although some countries are more advanced than others. The economic

activities in Africa are dominated by three countries, with Algeria, Egypt, and South Africa contributing 60 percent of the continent's gross domestic product (GDP), while the remaining countries share the other 40 percent. Seen in the light of emerging markets, African countries need a sound platform for corporate governance. According to Rossouw (2005), the need for corporate governance among listed and nonlisted companies and state-run enterprises is great. There are a number of factors that motivated a drive for sound corporate governance in Africa, for example:

- It is recognized that good corporate governance can contribute to the economic success of the country.
- It can enhance corporate responsibility and improve the reputation of companies.
- It can attract foreign investors.
- It is regarded as a deterrent to corruption and unethical business practice.
- It can ensure market discipline and transparency (Armstrong 2003, 25).

However, to grasp the real value of corporate governance requires an understanding of what the concept entails. This issue in the context of Africa will be discussed and measured, where possible, against previously performed studies by various researchers.

44.2 PURPOSE OF CORPORATE GOVERNANCE

According to the United Nations Economic Commission for Africa (UNECA 2002, 2), good corporate governance exists in those economies in which economic activity is unimpeded by corruption and other activities inconsistent with the public trust, and where the institutions of government:

- Have the capacity to manage resources efficiently
- Can formulate, implement, and enforce sound policies and regulations
- Can be monitored and be held accountable
- Have respect for the rules and norms of economic interaction

As such, from a government perspective, the key elements contributing to an environment of good corporate governance are transparency, an enabling environment for private sector development and growth, and institutional development and effectiveness (UNECA 2003, 2).

According to Rossouw (2003, 95), there are many obstacles in Africa that frustrate the quest for good corporate governance, such as:

- A general lack of effective regulatory and institutional frameworks
- A lack of market discipline and transparency, which is a deterrent for privately owned companies to list on the stock exchanges (where they do exist)

- A fear that the greater scrutiny of their corporate activities and the disclosure demands that go along with being listed can be exploited by the state and competitors
- Insufficient incentives for enterprises to list and thus enter the domain where standards of good corporate governance are required and enforced
- A poor example of good governance often set by state-owned enterprises, as their boards do not display either the competence or the independence that is required for good corporate governance

According to UNECA (2002, 3), in recognition that the responsibility for governance issues lies first and foremost with the national authorities, African states must commit to improving economic governance, for the following reasons:

- To enhance the ability to implement development and poverty reduction policies with scarce resources
- To execute public management functions in an accountable manner
- To create a credible policy environment in which domestic and international investors can have confidence and trade can be enhanced
- To strengthen absorptive capacity to attract and mobilize development assistance flows
- To demonstrate transparent and participatory economic policy making and execution as well as an open flow of information available to all stakeholders
- To signal an adherence to standards of institutional functioning free of corruption

According to Rossouw (2005, 96), there are various role players that are playing major roles to increase the levels of awareness and expertise with regard to corporate governance in Africa, such as:

- World Bank
- International Monetary Fund
- United Nations Development Program
- Commonwealth Association for Corporate Governance
- Organization for Economic Cooperation and Development

One of the corporate governance initiatives launched by various countries in Africa is the national codes of corporate governance, which are often driven by the private sectors and professional bodies. The countries that have published such codes of corporate governance include, for example:

- Ghana (Manual on Corporate Governance in Ghana, 2000)
- Kenya (Private Sector Corporate Governance Trust, 1999)
- Malawi (Corporate Governance Task Force, 2001)
- Mauritius (Report on Corporate Governance for Mauritius, 2003)

- Nigeria (Code of Corporate Governance for Nigeria, 2003)
- South Africa (Institute of Directors, 1994 and 2002—King Report)
- Tanzania (Steering Committee on Corporate Governance in Tanzania, 2000)
- Uganda (Manual on Corporate Governance Codes of Conduct, n.d.)
- Zimbabwe (Principles for Corporate Governance in Zimbabwe, n.d.)
- Zambia (Institute of Directors of Zambia, 2000) (Rossouw 2005, 97)

A number of African countries are in the process of developing these codes, indicating that they are serious about corporate governance. Many countries across the continent have adopted a code of corporate governance best practices based on international standards such as the South African King Report, the UK Cadbury report, the Organization for Economic Cooperation and Development Code, and the Commonwealth Secretariat Code (Nganga et al. 2003, 10).

Rossouw (2005, 101) states that the national codes all emphasize the ethical nature of good corporate governance, and special emphasis is placed on the fact that good corporate governance is based on the following fundamental values:

- Transparency
- Accountability
- Responsibility
- Probity

The various aspects of corporate governance that play a major role to realize these fundamental values are, for example:

- The importance of the role of the boards of the institutions
- Risk management
- Reporting and disclosure

In addition, corporate governance refers to the mechanisms through which corporations and their management are governed. As such, it involves a set of relationships among an organization's management, its board of directors, its shareholders, and its stakeholders. It furthermore provides the structure through which the objectives and the monitoring of performance are determined. To ensure sound corporate governance, the following are required:

- An established and seamless institutional and legal framework
- The pursuit of objectives that are supported by the board and management and that represent the interests of the organization and its shareholders

According to a study performed by Nganga et al. (2003, 9–12) on corporate governance in Africa, the following common issues were found:

- Courts remain slow and inefficient. Although most countries are reviewing their commercial laws to improve shareholder protection and corporate

governance principles, in practice the judicial systems remain slow and inefficient. For example, the current political situation in South Africa shows a negative trend in coping with the increase in crime and serious offenses. An example is a 42 percent increase in armed robberies in the past financial year (2005/06) in some of the major cities of South Africa, as published in the *Pretoria News* of September 30, 2006. There has also been an increase in other serious crime incidents reported, for example murder, rape, attempted murder, and carjacking. A potential result could be that investors will be hesitant to invest in South Africa (and other countries in Africa, as South Africa is regarded as one of the leading countries in Africa along with Egypt and Algeria); this could result in a negative economic growth, increase in poverty, and not benefiting from globalization. As such, it is clear that if these negative criminal offenses increase, the economic growth of Africa and South Africa can be seriously threatened.

Another example that could pose a serious risk for the South African business is the judicial system. Good corporate governance requires an independent judicial system that is impartial and free from interference, and renders respected judicial decisions. A recent event where a senior political figure was sentenced to prison for corruption and was escorted to prison by senior members of parliament indicated some sort of disrespect for the judicial system and reflecting a negative image and a high risk to potential investors.

- Most African countries are in a process of adopting an international governance code to deal with corporate governance.
- Stock market regulators have emerged as an alternative legal protection mechanism to inefficient courts. Listed companies represent a very small proportion of the total economic activity in the countries surveyed, with market capitalization-to-GDP ratios less than 20 percent in most countries; for example, according to Nganga et al. (2003, 10):

South Africa	123%
Egypt	25%
Morocco	26%
Nigeria	13%
Tunisia	12%
Botswana	24%
Mauritius	24%
Kenya	9%
Ghana	10%
Tanzania	4%

However, listed companies have the most developed regulation and corporate governance systems; they are subject to multiple layers of regulation

by the company law, the listing rules on stock markets, the market regulators, and the banking regulations for financial institutions. Due to the relatively slow and inefficient legal systems, these stock market authorities and regulators have emerged as the protection institutions for shareholders and minorities.

- There exists a general convergence to international accounting standards. According to Nganga et al. (2003, 11), listed companies in Kenya, Tanzania, Botswana, and Mauritius are required to use international accounting standards (IAS), while the Egypt generally accepted accounting principles (EGAAP) closely resemble the IAS. Morocco and Tunisia have accounting systems derived from French accounting standards. South African institutions also conform to GAAP and the IAS.
- Ownership concentration is high. There is a high level of ownership concentration on most stock markets where owners have sidestepped owner-manager agency problems by acquiring a controlling stake in businesses. For example, in Kenya the top five companies represent over half the market capitalization and all have a multinational as the controlling body. Family control is of a particular concern in Egypt and Mauritius, where families have historically been very influential in business (Nganga et al. 2003:12).
- There is low awareness among shareholders and directors. Nganga et al. (2003, 12) state that while corporate governance standards have been updated in Africa, there remains a lag in awareness among shareholders and directors. However, most countries are aware of this problem and address it in their codes of corporate governance, such as South Africa in the King Report on Corporate Governance of 2002.

The role of the directors is probably one of the most important issues of an effective corporate governance code. When analyzing the King Report, for example, this issue becomes apparent, as will be discovered in the next section.

44.3 ROLE OF THE BOARD

Organizations should have a unitary board of directors that can both lead and control the organization. It should comprise directors with diverse backgrounds, skills, and experience. The board should also have a charter formalizing its responsibilities. The following responsibilities are envisaged for a board:

- Appoint the chief executive officer.
- Provide strategic direction and identify key risk areas.
- Enforce internal control policies and procedures.
- Determine the appropriate remuneration levels of directors.
- Comply with all relevant laws, regulations, and codes of conduct.
- Appoint external auditors to review/monitor the accounting and reporting systems.

- Ensure that the systems of internal control are functioning effectively.
- Provide open and timely communication to all relevant stakeholders.

The general responsibilities of the board, as discussed by the King Report of 2002, are in agreement with the aforementioned responsibilities. According to the report, the board of an organization and its management have two main responsibilities:

1. To shareholders to ensure the maximizing of long-term benefits in terms of profits, cash flows, and minimizing risks
2. To other stakeholders to maximize wealth and to ensure the sustained prosperity of the business

Every board should have a charter setting out its responsibilities, which encompass adoption of strategic plans, effective control and monitoring of operational performance and management, determination of policy and procedure to ensure the integrity of the organization's risk management and internal controls, communications policy, and director selection, orientation, and evaluation. The board must ensure that material decisions remain within its jurisdiction.

Another aspect that is prominent and requires attention when developing a code for corporate governance is that of risk management.

44.4 RISK MANAGEMENT

Many developing and transitional economies, such as those of African countries, recognize the fact that a healthy and competitive corporate sector is necessary for their sustainable and shared growth and that corporate governance is fundamental for the private sector. As African countries endeavor to attract a share of foreign investments, they have to assure investors that their investments will be secure and efficiently managed on the basis of a transparent and accountable process. Effective risk management can be regarded as one method of providing assurance of a sound investment to investors. The King Report (2002) also initiated the development of a corporate governance framework for risk management. The purpose of the King Committee was to promote the highest standards of corporate governance in South Africa. According to the King Committee (2002, 96) report, risk frameworks, as part of an organization's corporate governance, must provide assurance with regard to:

- Effectiveness and efficiency of operations
- Safeguarding of assets
- Compliance with applicable law
- Business sustainability
- Reliability of reporting and
- Behaving responsibly toward stakeholders

In terms of risk management, the King Committee (2002, 98) states that the board has the following responsibilities:

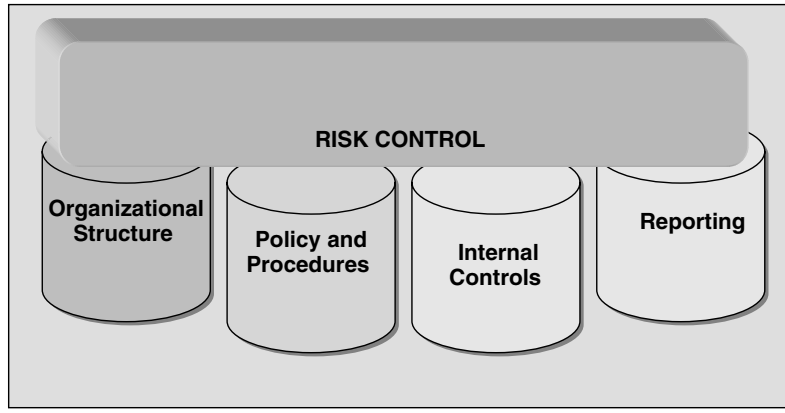
- To ensure that processes and outcomes of key risk indicators are undertaken on an annual basis
- To appoint a board committee or an appointed dedicated committee that should review the risk management process and the significant risks facing the company
- To disclose risk management in the annual report
- To ensure that the internal audit function provides an independent assurance that the internal controls ensure effective risk management
- To ensure that there is compliance with the applicable regulations

One of the fundamental components of an effective risk management framework is the control of the risk exposures. According to Young (2006, 94), control measures for risk are based on four pillars, illustrated in Exhibit 44.1.

The organizational structure will ensure that specific roles and responsibilities are allocated for effective risk management, which is a specific corporate governance requirement.

Policies and procedures, the second pillar, are imperative for risk management in order to provide consistency and discipline within an organization and ensure the overall defining and allocating of specific roles and responsibilities for managing risk.

Internal controls should be established to ensure the effectiveness of policies and procedures, which is another sound corporate governance requirement.



Source: Young (2006, 94).

EXHIBIT 44.1 PILLARS OF RISK CONTROL

The Basel Committee (1998, 6–7), for example, identified five types of control breakdowns that have led to substantial losses for banks:

1. A lack of adequate management supervision and accountability, and failure to develop a strong risk management culture within the bank
2. Inadequate assessment of the risk of certain banking activities, whether on or off the balance sheet
3. The absence or failure of key control activities, such as segregation of duties, approvals, verifications, reconciliations, and reviews of operating performance
4. Inadequate communication of information between levels of management within the bank, especially in the upward communication of problems
5. Inadequate or ineffective audit programs and other monitoring activities

These control breakdowns are typically issues that a well-structured corporate governance and risk management framework will address.

Risk reporting, the fourth risk control pillar, is the process whereby an organization reports on risk internally, through its management information system, and externally, to its regulators and shareholders (Young 2006, 100). This is also an important corporate governance requirement that will assist in effective decision making. According to UNECA (2002, 12), a major element of good corporate governance is effective participatory decision making. This issue poses a risk to a number of African countries when considering, for example, the local elections. It is stated that the smooth running of elections is still problematic in several African countries, with scores of people invariably being disenfranchised, leading to poor risk management and corporate governance (UNECA 2002, 12).

Considering the aforementioned and comparing it with the requirements of good corporate governance (namely, that it involves a set of relationships between an organization's management, its board, its shareholders, and its other stakeholders and provides the structure through which the objectives and the monitoring of performance are determined), it is evident that there is a direct correlation between effective risk management and corporate governance.

It is, furthermore, clear that if an organization, like a bank, can provide assurance of complying with the aforementioned governance requirements, it would most likely attract the attention of potential investors.

44.5 REPORTING AND DISCLOSURE

Every company should report at least annually on the nature and extent of its social, transformation, ethical, safety, health, and environmental management policies and practices. The board of directors should, in determining what is relevant for disclosure, take into account the environment in which the company operates—for example, appropriate HIV/AIDS strategy (e.g., according to the Pan-African Consultative Forum on Corporate Governance [2001, 12], on average

6,500 Africans die of AIDS-related illnesses each day). Corporate governance is a set of rules that also focuses on transparency of information and management accountability. It imposes fiduciary duty on management to act in the best interests of all shareholders and properly disclose operations of the organization. Improved management accountability and transparency will fulfill investors' expectations of and confidence in management and corporations and in return increase the value of the organization.

According to Rossouw (2005, 100), all reports should propose an outline of what stakeholder engagement should entail. The process should commence with the identification of stakeholders and then be followed by a policy that formulates how the organization will communicate with its shareholders. Rossouw (2005, 100) states that the Zimbabwean code goes even further and recommends that a code of conduct should be developed for stakeholder engagement that will ensure that the rights of stakeholders are protected (Principles for Corporate Governance in Zimbabwe, n.d.).

Although the emphasis of disclosure and reporting is on stakeholder communication, the general reports lack rigor and discipline in most African countries, although there are exceptions such as the Kenyan code and the King Report for South Africa (Rossouw 2005, 100).

44.6 CONCLUSION

A sound code of corporate governance should ensure that the following are achieved:

- A definition of the organization's objectives and strategies and the means to implement them
- Assurance that the needs and requirements of all stakeholders are met
- Clear defined principles regarding standards of conduct
- A sound risk management framework

It is evident that by complying with the basic requirements of good corporate governance, any organization will have a structured platform for effective operational risk management. This will ensure efficient mobilization and allocation of capital, the efficient monitoring of corporate assets, and the effectiveness of overall corporate performance.

Although African countries across the continent are at various stages of implementing corporate governance codes and principles, most of these initiatives are being hampered by problems of corruption, inadequate infrastructures, and cumbersome bureaucratic procedures. Corruption can be regarded as one of the factors that restrict effective corporate governance in Africa. Grand corruption, for example, tends to involve leaders, politicians, senior bureaurocrats, and entrepreneurs. This can take many forms, such as bribes—for example, South Africa's defense contracting in 2001 allegedly involving top businessmen and senior politicians.

However, apart from the constraints of complying with good corporate governance principles, the implementation of sound risk management practices, especially, will add value to the initiatives to improve the capacity of African countries to adapt and apply the relevant codes and standards for sound corporate governance.

References

Basel Committee on Banking Supervision. 1998. *Framework for Internal Control Systems in Banking Organizations*. Basel: [s.n.], September 1998.

Basel Committee on Banking Supervision. 2003. *Sound practices for the management and supervision of operational risk*. Basel: Bank for International Settlements, February.

Basel Committee on Banking Supervision. 2004. *International convergence of capital measurement and capital standards: A reviewed framework*. Basel: Bank for International Settlements, June.

King Committee and Commission on Corporate Governance. 2002. *King 2 report on corporate governance for South Africa: Draft for public comment*. Pretoria: Institute of Directors in Southern Africa.

Pan-African Consultative Forum on Corporate Governance [2001, 12], http://www.ifc.org/ifcext/cgf.nsf/AttachmentsByTitle/Pan_Africa_2003_Summary_Report/$FILE/PACFCG+SUMMARY+CONFERENCE+REPORT.pdf.

Rossouw G. J., *Business Ethics and Corporate Governance in Africa*, University of Pretoria, Sage Publications, 2005.

South African Financial Sector Charter, August 2002.

United Nations Economic Commission for Africa. 2002. *Guidelines for enhancing good economic and corporate governance in Africa*.

Young, J. 2006. *Operational risk management: The practical application of a qualitative approach*. Pretoria: Van Schaik Publishers.

CHAPTER 45

EUROPEAN UNION—REGIONAL GUIDANCE

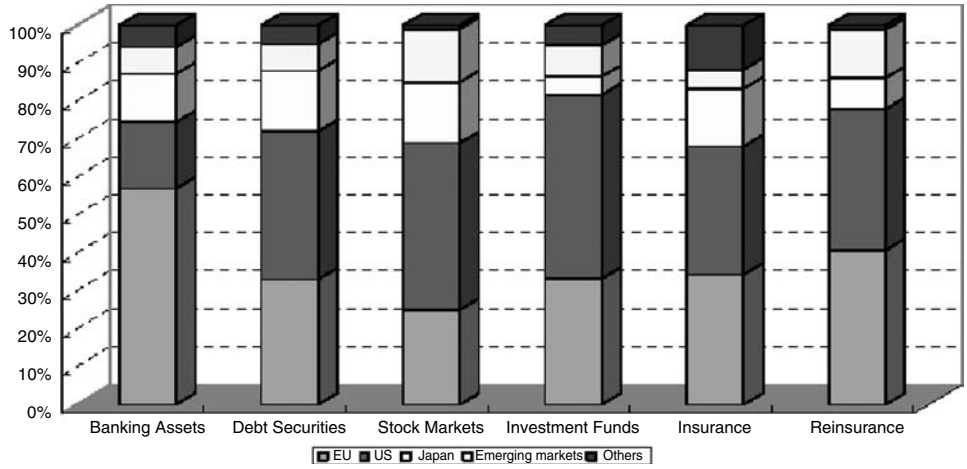
Michael Mainelli

45.1 INTRODUCTION

A survey of compliance for the 27 European Union (EU) countries and two candidate countries, Turkey and Croatia (as of January 2007), must, of necessity, be shallow. The EU financial services industry is undergoing great changes, and the regulatory and compliance implications are equally great.

The EU has a 20 percent to 40 percent global market share of various financial services. Working from data from the International Monetary Fund (IMF), the World Federation of Exchanges, the Bank for International Settlements, the European Fund and Asset Management Association, and company reports of the top 100 global reinsurers, the EU estimated the global market shares in commercial bank assets, debt securities, stock market capitalization, investment fund net assets, life and nonlife premiums and nonlife net written premiums in reinsurance for the EU in 2004. (See Exhibit 45.1.)

Estimates of something as fungible as financial services must be treated cautiously but, overall, the EU financial services industry is comparable to that of the United States. The EU has a larger share of the global banking market (45 percent) and global reinsurance (nearly 40 percent), while the United States



Source: Commission of the European Communities, ''Financial Integration Monitor 2006,'' SEC (2006), 1057, Commission Staff Working Document, Brussels, July 26, 2006, 6. http://ec.europa.eu/internal_market/finances/docs/cross-sector/fin-integration/060728fim_en.pdf.

EXHIBIT 45.1 EU SHARE OF WORLD FINANCIAL ACTIVITY 2004 (PERCENT)

has a larger market share of stock market activities (40 percent) and investment management (50 percent) sectors. All these market shares are fluid. Changes in the United States, particularly due to regulation, make the EU more competitive for wholesale financial services, while the EU's fragmented retail financial services serve as a barrier to entry against efficient foreign firms. Given the EU's population of 480 million in 2007, the EU will remain a major domestic retail financial services market regardless of the skill or incompetence of regulation or compliance, so this chapter will focus on areas where regulation will help the EU to gain or lose significant international business.

45.2 THE ROLE OF THE SINGLE MARKET

The EU began as a Common Market and in many ways is defined by the members' desire to eliminate trade barriers and simplify rules to enable individuals, consumers, and businesses in the EU to make the most of the opportunities offered to them by having direct access to this enormous market.

The single market is based on four freedoms enshrined in treaties among the members—the free movement of people, goods, services, and capital. Financial services affect all four freedoms. People need payment, savings, and protection products that transcend national boundaries. Movement of goods and services benefits from efficient, integrated payment systems. The efficient allocation of capital across the EU should benefit growth for all members. EU policy and

strategy in financial services and financial markets tries to promote coherence and consistency among banking, insurance, securities and investment funds, financial markets infrastructure, retail financial services, and payment systems. To quote from the EU web site:

> From 1999 to 2005, this overarching policy was delivered in the framework of the Financial Services Action Plan (FSAP), and the Commission continues to regularly monitor progress made in implementing the FSAP, for instance through making twice-monthly updates to its FSAP transposition tables. Work also continues on co-ordinating the initiatives driven by the FSAP, including the restructured financial services committee architecture (Lamfalussy approach), the Inter-institutional Monitoring Group, and supervisory convergence. In December 2005, the Commission published the White Paper on Financial Services 2005–2010, which sets out the Commission's objectives in financial services policy for the period to 2010.

EU objectives that affect compliance are threefold. First, the EU intends to remove barriers to financial services, including *reducing* unnecessary compliance obligations. The EU is looking to allocate capital more appropriately and reduce the costs of financial services. Second, the EU intends to enforce existing regulations, *balancing* the compliance drivers of financial stability and consumer protection with the markets through rigorous impact assessment. Third, EU relations with other global financial marketplaces and strengthening European influence globally require *enhancing* supervisory cooperation and convergence within the EU. The net impact of this third point is likely to be an increase in compliance obligations.

In 2001, the EU promoted a new approach to financial services regulation, the Lamfalussy Process, named after the chair of the EU advisory committee that created it, Alexandre Lamfalussy. There are four levels to the Lamfalussy Process. At the first level, the European Parliament and Council of the European Union adopt new legislation, establish the core values of a law, and build guidelines for implementation. The law then progresses to the second level, where sector-specific committees and regulators advise on technical details. At the third level, national regulators coordinate new regulations with other nations. The fourth level consists of compliance and enforcement of the new rules and laws. The Lamfalussy Process is intended to provide more consistent interpretation in national supervisory practices, and provide better interpretation and application of legislation. A good example of the Lamfalussy Process in action is the current implementation of the Markets in Financial Instruments Directive (MiFID). MiFID was implemented in 2007 and is expected to change trade transparency significantly and ensure best execution.

EU policy normally divides the financial services sector into three major areas: banking, insurance, and investment and securities. However, there are two distinct areas of compliance within the EU for all three areas (i.e., another divide is between retail financial services and wholesale financial services).

45.3 DIVIDE AND CONFLICT—RETAIL AND WHOLESALE

Retail financial services are characterized by a tremendous amount of national legislation about how products can be sold, marketed, or distributed, ostensibly for consumer protection. With 27 countries and numerous regulators in many countries, there are several hundred regulatory organizations involved. EU or national interpretations of international regulation (e.g., anti-money laundering) can have a significant effect on retail financial services. EU legislation has removed interest rate controls, capital controls, and segregated markets (e.g., allowing banks to offer insurance). But implementation is frequently patchy and inconsistent, for example on the Second Money Laundering Directive (2MLD); "the failure of 2MLD to provide for the establishment of competent authorities in each Member State to monitor and enforce compliance with the directive requirements means that compliance varies widely, not only between Member States but also across business sectors within Member States."[1]

Wholesale financial services are global; thus compliance is complicated where national, EU, and international regulation meet each other, ranging from International Financial Reporting Standards (IFRS) to Basel I and Basel II or anti-money laundering regulations. Many of the European wholesale markets are recent. London's Big Bang, the removal of barriers to entry for its capital markets, was as recent as 1986. Wholesale financial services are mobile and, for a variety of reasons, increasingly centered around London as one of the two global financial centers alongside New York City.[2] Because wholesale markets are competing globally and are mobile, a lot of debate focuses on whether London remains competitive with non-EU wholesale markets, particularly when retail and wholesale regulation conflict, for instance with national capital markets legislation or the treatment of corporations or anti-money laundering. Discussions with numerous wholesale market firms indicates that several are beginning to see "effective implementation of compliance" as a competitive tool. If they can implement credible systems that prove to regulators they comply with regulations before their competitors, they shift the burden of regulation to the competition. For example, considering MiFID "best execution" requirements (though Regulation National Market System or RegNMS "best execution" requirements in the United States are comparable), firms have been discussing how they might develop generalized compliance systems that would apply to anticipated new regulation using dynamic anomaly and pattern-recognition techniques.[3]

At the retail level, the introduction of the euro (€) since 2000 has accelerated moves toward more standardization of retail regulation, both because products are more comparable and because a common, stable currency has increased the mobility of capital. The EU continues to push for further currency integration in the form of a single euro payments area (SEPA). SEPA aims to enable European citizens to make payments in the euro area as securely, quickly, and efficiently as payments within national borders. Service levels for domestic and cross-border retail payments are to be identical by 2010. The introduction of IFRS[4] across

7,000 listed firms in the EU is leading to pressure to align IFRS accounts with corporate tax returns. Disclosure quality is increasing and, in turn, this is leading to increasing pressure for the harmonization of taxation conventions, and perhaps increasingly for a harmonization of taxation rates across the EU.

45.4 LONDON VERSUS BRUSSELS

At the wholesale level, the most important discussions seem to be between Britain's Financial Services Authority (FSA) and the EU—that is, London versus Brussels. Britain's move to a unitary regulator for all financial services, wholesale and retail, international and domestic, insurance and banking, was controversial when it began in the 1990s. However, the FSA is widely seen as, on balance, a success. The FSA has particular support from the wholesale financial services industry, which views it as an ally both in dealings with the EU in Brussels and with other regulators abroad. In particular, the FSA is seen as a strong ally in discussions with the large range of U.S. wholesale finance regulators.

Despite all the good words about the regulatory system in the UK, the FSA does have a track record of "super-regulating," and the implementation of several EU directives has been more rigorous in the UK than in other EU member states. The Third Anti-Money Laundering Directive and the Insurance Mediation Directive are two recent examples of FSA super-regulation in relation to other European jurisdictions. The British Institute of International and Comparative Law recently noted[5] that the Insider Dealing and Market Abuse directive is another example of different levels of regulation resulting from the same directive.

The FSA is, however, now gaining a reputation for the rigor with which it undertakes impact assessments and cost/benefit analyses of proposed regulation, and, as the European Policy Forum notes:[6]

> The EU Directors of Better Regulation Group have analyzed the way in which RIAs operate in ten member states. It has noted that overall best practice is found in the United Kingdom.

Aspiring financial centers can learn a great deal from the contrast between UK and U.S. financial services regulation. It was not always like this. Back in the late 1990s—when the arguments over whether Britain should join the single European currency were raging—the City was seen as a trump card by pro-Europeans. Lord Levene stated in 1998 that if Britain stayed out of the euro for too long, "London's business will, in time, be eroded." The British government was worried enough to make the impact of the euro on the financial services industry one of the "five tests" that would decide if the UK joined the euro. The idea that the City of London and Brussels were natural allies seemed to make sense. Few markets are as global as the wholesale financial markets of the City of London. Almost 25 percent of its employees are citizens of other countries. Yet gauging the City's attitude toward Brussels is difficult. Open Europe, a Eurosceptic lobby group, and Business for New Europe, a Europhile

group, can both identify City sponsors. There is more talk of "London versus Brussels" as the UK being out of the euro zone has had little detrimental effect, the City increasingly attracts non-EU business, and the City prefers light legislation over the "one size fits all markets" approach of Brussels.

London's unitary regulator might be a liability if, driven by the breadth of its remit, it allows specific competitive centers to pick off specific subsections of the financial services industry (e.g., insurance captives, private banking, or hedge funds). Further, one can anticipate more of the extraterritorial regulatory disputes that have already been seen over subjects such as the acquisition of European exchanges by American exchanges or the Unlawful Internet Gaming Enforcement Act.

45.5 THE VESTED INTERESTS

As in so many other areas of policy by the EU's national members, the simple and seductive argument for national champions starts with "finance is so important that it must be treated differently." There are legitimate concerns justifying special treatment, particularly consumer confidence, which despite the common market remains astonishingly parochial; taxation, where financial services support taxation collection; and pensions, where an underfunded industry would lead to significant future demands on an EU member state.

Financial cartels, such as the various national retails banks or national fund industries, do not like liquid markets that turn financial services into commodities. Numerous studies have lamented the lack of competition for retail financial services within member states.[7] The top five banks in most EU member states hold over 50 percent of the market. Only in Germany do the top five banks hold less than 25 percent of the market. "Despite all the laws and rules enacted since the mid-1980s to give the European Union a single market in goods and services, including banking and finance, banks have obstinately gone on getting bigger within their home countries. They have merged at home much more enthusiastically than they have merged or branched or sold services across borders."[8]

In the wholesale markets, two antithetical models complicate things for regulators. The first model is that financial services needs vertical integration in order to achieve efficiency, for example linking trade execution through to clearing and settlement (e.g., Deutsche Börse). The second model is that of horizontal competition at various strata in the supply chain, for example the London Stock Exchange competing with Euronext on trading, while Euroclear competes with SegaInterSettle on clearing and settlement. The two models conflict and raise conflicting monopoly control issues, for example preventing the London Stock Exchange from owning Crestco, or hampering financial exchanges' mergers and acquisitions.

Looking at progress in core financial services can be disheartening. Change is slow. However, in other areas the EU financial services industry is undergoing rapid change. One example is private banking, where, for example, legislative

changes are bringing wealth management services back onshore in Belgium. Another example is gambling, particularly onshore gambling. The scale and influence of gambling in Europe is often not appreciated, particularly in the United States.[9] First, gambling is a large market in its own right—in less than a decade Betfair in the UK has become, arguably, the largest exchange in terms of transaction volumes. Second, gambling in financial instruments is an important link from consumers to wholesale financial markets, for a variety of tax and regulatory reasons. Because of the United States' 2006 Unlawful Internet Gambling Enforcement Act, which effectively outlaws online gambling in the United States, European online gambling regulation and compliance is in turmoil as many of its customers are from the United States and many payment systems rely on U.S. providers.

45.6 INTERNATIONAL REGULATORY COMPETITION

Cities around the world compete to have businesses located in their city. Wholesale financial services is an attractive business sector both because it is hot—financial services has been a rapidly growing and successful sector for the past quarter of a century—and because it is highly mobile—therefore potentially influenced significantly by policy and planning. The importance of financial services as a topic for government officials and regulators can be felt in this excerpt from a UK HM Treasury Report:[10]

> London is, on many counts, the world's leading financial center. . . . London is unambiguously the world's largest centre for international financial services because, unlike the domestic focus of other large financial centres, it dominates key international financial markets and, for example, has more foreign banks than any other financial centre. Britain's other important financial centres, primarily in Edinburgh and Leeds, contribute to London's international reputation and strength. . . . London's competitiveness across a wide range of international wholesale markets is based around its three key strengths:
>
> - scale: the size of London's markets creates genuine liquidity, the cornerstone of an efficient market;
> - scope: nowhere else in the world has London's range of services, or London's record for innovation in new services like derivatives and Islamic finance; and
> - internationalism: London has a tradition of openness with regard to foreign ownership and participation, historical links with emerging markets in Asia and the Middle East, and a strong transatlantic relationship.

Some of the analysis spills over into almost a parody of determinism or Haeckel's belief that "ontogeny recapitulates phylogeny"; that is, to develop as successfully as London, a city must be London:

> An economic legacy of freedom, flexibility and openness: London's historic legacy is one of internationalism and of trade. Its financial markets provide

> a bridge between the time zones of Asia and America. While English has become the unquestioned global business language, clarity and certainty of English law has meant that it has also become the legal language of choice for much international commerce. British attitudes to trade and foreign ownership are founded in traditions of openness and fair play, and policies towards migration and temporary foreign workers are some of the fairest and most flexible in the world.[11]

Comparative financial center research interests journalists seeking to create a story of rivalry between London and New York City. In many articles on both sides of the Atlantic the seesaw of competitiveness is seen as tilting in London's favor due to regulation:

New York City view:

> [New York City's] Economic Development Corporation said yesterday it is hiring McKinsey and Company for $600,000 to formulate a strategy for New York City to maintain its title as financial capital of the world. . . . The hiring comes as London has gained ground on Wall Street in recent years, experts say, with expanding European markets, an explosion of activity in the hedge fund business and an increasing number of companies that are choosing to go public on the London Stock Exchange, as opposed to in New York. Some say that London is benefiting from America's Sarbanes-Oxley Act of 2002, sweeping legislation that created new corporate governance, financial disclosure, and public accounting standards for companies. Critics said the legislation increased the cost of doing business here.[12]

London view:

> London is overtaking New York and is re-establishing itself as the world's financial centre for the first time since the days of Empire.[13]

45.7 ONE WORD—REGULATION, REGULATION, REGULATION

Much research has reported fears about overregulation, such as the Centre for the Study of Financial Innovation (CSFI)'s banking survey in 2005:

> The UK Government has taken financial services for granted, and any unwarranted tightening of regulation will kill the golden goose. The regulatory industry has grown bigger without growing smarter.[14]

In the 2005 Z/Yen study for the City of London Corporation,[15] more than 80 percent of respondents saw the regulatory environment as very or critically important. Respondents from outside the UK placed greater emphasis on the regulatory environment, with 57 percent considering it critically important compared with 39 percent in the UK. Just over 60 percent of international bankers saw the regulatory environment as critically important, compared with 35 percent of UK bankers. The regulatory environment is considered much better in

London and New York City than it is in Paris and Frankfurt. Over 90 percent of respondents rated the regulatory environment in London as good or excellent.

Many economists have long talked about potential competition between regulatory regimes. A continuing debate in financial services in Europe has been between those who believe that lighter regulation will increase the scale of the business versus those who believe that stronger regulation will increase the scale of the business. Both sides have invoked both versions of Gresham's Law—"good money drives out bad" and "bad money drives out good" [Mundell, 1998].[16] It must be gratifying for economists to see the cause of potential relocation attributed so directly to regulation:

> London's Mayor Ken Livingstone recently visited New York City, trolling for businesses that might relocate jobs and investment activity from the United States to Great Britain. Asked what he considered London's competitive advantage over New York, he replied, "Sarbanes-Oxley."[17]

One of the reasons that London is a direct competitor of New York City is the regulatory environment in the two cities.

> Some would like the SEC (the Securities and Exchange Commission in the USA) to become more like Britain's super-regulator, the Financial Services Authority (FSA). The FSA has won plaudits for an approach based more on principles rather than hard rules. It prefers to nudge rather than bully. Moreover, it is widely considered to be better at analysing the potential costs and benefits of proposed regulatory changes.[18]

The regulatory environment is second only in importance to the availability of skilled personnel when locating wholesale financial services. There are two sides to the regulatory environment, the quantity and rigor of the regulations themselves and the way in which firms are expected to comply. Many people are critical of the United States' heavy-handed approach to regulating financial services. Some regulators, such as the SEC, adopt a prescriptive, rules-based approach, while the FSA has a less prescriptive, principles-based approach. As the *Economist* reports:

> In 2004 the Financial Services Authority responded [to concerns about regulation] by setting up a separate division for wholesale and institutional markets, headed by Hector Sants, previously an investment banker. "We recognise," says Mr Sants, "that good regulation is a key component of a successful marketplace." The FSA is now highlighting the need for regulation to be based on principles rather than detailed prescriptions.[19]

John Tiner, the chief executive of the FSA, states:

> We probably already have too much regulation. What we need to head towards is better regulation.[20]

While many in London still think the FSA is heavy-handed in its approach, the UK almost certainly benefits from the FSA's comparatively mature approach. It can be argued that there are two serious regulatory problems facing the United States. First, the SEC is good at enforcing regulations but has lost sight of its other goal—to ensure that markets run smoothly and efficiently. Second, the regulatory structure has too many agencies. There are four separate banking regulators, and the multiple state and federal regulators continuously "tread on each other's toes."

It would appear that the United States has scored another regulatory own-goal with Sarbanes-Oxley legislation. The London Stock Exchange has been a big beneficiary of the legislation with international firms flocking to list in London (either on the main market or on AIM) rather than listing in the regulation-bound United States (London hosted 172 international listings in the first nine months of 2006 compared with 134 in New York[21]).

It is possible to overstate the detrimental effect of one piece of legislation and forget other sources of competitive disadvantage. A detailed study into the cost of raising capital in various markets[22] reported recently that, although significant, the cost of Sarbanes-Oxley compliance was not the biggest cost involved in raising capital. The biggest cost was the high fees charged by Wall Street banks (6.5 percent to 7 percent of the value of shares offered against a typical level of 3 percent to 4 percent in Europe).

45.8 THE FUTURE OF REGULATION

Regulation within financial services is generally the result of a knee-jerk reaction to an acknowledged problem that is perceived to be facing the industry. There are generally two forms of financial regulation: legal and self-regulated. Legal regulation emanates mostly from EU directives being made into national laws, though member states still add local requirements. Compliance imposed with the general support of the regulated, but without legal sanction—self-regulation—has been out of favor, but is returning as regulators and the financial services industry realize that "one size fits all" harms competition and consumers.

Regulation is important. Business is transacted where regulators permit, but also where people trust the regulators. Over time, regulators either gain the skills to regulate international financial transactions and institutions or lose credibility by being too intransigent or too lax. Sooner or later, certain regulatory regimes pull away from the pack or, sometimes more accurately, others drop away.

The financial services industry has been at the center of regulation for centuries. Given this level of experience in compliance and regulation, it would be nice to be able to say that regulation was generally well thought through and fit for purpose. Unfortunately this is generally not the case. A short review of EU regulation cannot begin to explain the intricacies of regulations in, for example, retail lending, data protection, competency requirements, capital requirements, market access, marketing, and web sites disclosure or reporting requirements.

45.9 A NEW APPROACH

Quality in products and services is now a widespread European expectation. Third-party conformity assessment services have been steadily growing in response to the increasing need for impartial and transparent demonstration of the conformity of products and services exchanged in the European market. Regulators, industry, and society place confidence in these services particularly through meeting the requirements of European Directives and Regulations. A Council Resolution (2003/C 282/02) in November 2003 acknowledged the importance of New Approach and Global Approach directives that place much more reliance on conformity assessment as opposed to regulation, along with the need for clearer framework for accreditation and conformity assessment. This approach may have important implications for financial services.[23]

Since 1987 some 25 directives, outside of financial services, have been adopted on the basis of the New Approach and the Global Approach. These directives have the dual purpose of ensuring the free movement of goods through technical harmonization of entire product sectors, and of guaranteeing a high level of protection of public interest objectives referred to in Article 95, paragraph 3, of the EC Treaty. Innovative features of this legislative technique include the definition of mandatory essential requirements, the setting up of appropriate conformity assessment procedures and the introduction of CE marking. Business and industry are given a wide choice of how to meet their obligations. The European standards bodies have the task of drawing up technical specifications which offer one route to complying with these essential requirements.

> Where Member States decide to operate accreditation, they shall establish or have established and maintained under their jurisdiction a national accreditation body. Where accreditation is not operated by the public authorities themselves, Member States shall entrust the national accreditation body with the operation of accreditation as a public authority service and grant it formal recognition on behalf of government, authorising it to operate accreditation under the authority of the public authorities. Considering the added value of accreditation to serve as the last and authoritative level of control of conformity assessment activities with regard to technical competence in order to create mutual confidence, Member States shall ensure that accreditation operates free from commercial competition and shall entrust its operation to a single national accreditation body.

Accreditation will in future provide the basis for the recognition of conformity assessment bodies attesting conformity to the requirements of European directives and regulations. The European Commission's New Approach is that accreditation will be defined as a service of general interest, representing the last authoritative level of control of the conformity assessment services delivered both in the voluntary sector and, in the future, in the regulated sector. The European Commission expects increased transparency, coherence, and cooperation in both the regulatory and voluntary areas for New Approach directives.

New Approach directives are based on the following principles:

- Harmonization is limited to essential requirements.
- Only products fulfilling the essential requirements may be placed on the market and put into service.
- Harmonized standards, the reference numbers of which have been published in the Official Journal and which have been transposed into national standards, are presumed to conform to the corresponding essential requirements.
- Application of harmonized standards or other technical specifications remains voluntary, and manufacturers are free to choose any technical solution that provides compliance with the essential requirements.
- Manufacturers may choose between different conformity assessments procedures provided for in the applicable directive.

It may well be that the Lamfalussy Process will be subsumed within the New Approach being used for other products and services. In such a complex, federal structure, the future of regulation and compliance within the EU will never be straightforward. Nevertheless, there is clear recognition that a balance in regulation is needed to ensure vibrant markets, that legislation is not the only answer, and that the regulatory system must continue to evolve wherever possible by applying principles with pragmatic enforcement. When contrasted with the legalistic and rules-based approaches in the United States, the EU has a lot to inspire other regulatory regimes.

Notes

1. British Institute of International and Comparative Law, "Comparative Implementation of EU Directives (II)—Money Laundering," City of London Corporation Research Series, no. 10 (December 2006).
2. Mark Yeandle, Michael Mainelli, and Adrian Berendt, "The Competitive Position of London as a Global Financial Centre," Corporation of London, November 2005.
3. Michael Mainelli and Mark Yeandle, "The Best Execution: Trader or Client?," *Fund AIM* 1, no. 1, Investor Intelligence Partnership (January 2007): 43–46.
4. Holger Daske and Günther Gebhardt, "International Financial Reporting Standards and Experts' Perceptions of Disclosure Quality," *Abacus* 42, no. 3/4, 461–498.
5. British Institute of International and Comparative Law, "Comparative Implementation of EU Directives (I)—Insider Dealing and Market Abuse," Corporation of London, December 2005.
6. European Policy Forum, "Rebalancing UK and European Regulation," Corporation of London, April 2005.
7. Stephen Martin and Michael Mainelli, "Why Bother to Be Better? Strategically Stagnant Personal Current Accounts," *Journal of Strategic Change* 12, no. 4 (June–July 2003): 209–221.
8. "Survey: International Banking—What Single Market?," *Economist*, May 18, 2006.

9. Michael Mainelli and Sam Dibb, "Betting on the Future: Online Gambling Goes Mainstream Financial," Centre for the Study of Financial Innovation, no. 68, December 2004.
10. HM Treasury, "Financial Services in London: Global Opportunities and Challenges," (March 2006).
11. HM Treasury, "The UK Financial Services Sector: Rising to the Challenges and Opportunities of Globalisation," March 2005.
12. David Lombino, "Firm Hired to Boost City's Competitive Edge versus London," *New York Sun*, September 27, 2006.
13. John Arlidge, "The Golden Gateway," *Sunday Times Magazine*, December 3, 2006, 60–70.
14. Centre for the Study of Financial Innovation, "Banking Banana Skins," Centre for the Study of Financial Innovation, 2005.
15. Yeandle, Mainelli, and Berendt, "Competitive Position of London."
16. Robert A. Mundell, Uses and Abuses of Gresham's Law in the History of Money, Zagreb Journal of Economics, Volume 2, No. 2, 1998.
17. Kathryn Wylde, president and CEO of the Partnership for New York City, *New York Post*, August 3, 2006, www.nycp.org/webNews/2006/web_080306_strangling percent20nyc .html.
18. "Down on the Street: A Special Report on America's Capital Markets," *Economist*, November 25, 2006, 97.
19. "Capital City," *Economist*, October 21, 2006, 99–100.
20. *Daily Telegraph*, September 13, 2006.
21. "How to Protect an Industry," *Economist*, October 21, 2006, 13.
22. Oxera Consulting Limited, "The Cost of Capital: An International Comparison," Corporation of London, June 2006.
23. Michael Mainelli, "Standard Differences: Differentiation Through Standardisation?" (ISO9001, SAS70 and management systems), *Journal of Risk Finance*, The Michael Mainelli Column, Volume 6, Number 1, pages 71–78, Emerald Group Publishing Limited (January 2005).

References

Armstrong, P. 2003. Status Report on Corporate Governance Reforms in Africa. Johannesburg, South Africa: Pan-African Consultative Forum on Corporate Governance.

Economic Commission for Africa. 2002. Guidelines for Enhancing Good Economic and Corporate Governance in Africa. UNECA Final Draft May 2002.

Nganga, S. V. Jain, and M. Artivor, 2003. Corporate Governance in Africa: A Survey of Publicly Listed Companies. CGIA, December 2003.

Rossouw, G. J. 2005. Business Ethics and Corporate Governance in Africa. University of Pretoria. Sage Publications.

CHAPTER 46

CORPORATE GOVERNANCE IN MAJOR ISLAMIC NATIONS

Anthony Tarantino, PhD

46.1 INTRODUCTION

Western notions of corporate governance are rooted in improving shareholder value and are, in many cases, overly concerned with short-term gains at the expense of longer-range goals. Social responsibility and good corporate citizenship are often mentioned in corporate literature, but are rarely a driving force. The concepts of good governance and best practice standards developed after a series of painful scandals typically look to improve ethical behavior, transparency, and accountabilty. Even with these improvements, there remain three areas in which Western notions of corporate governance will fall short of Islamic requirements for moralistic behavior:[1]

First, Western business concepts of ethics and morality are typically socially and secularly based humanistic values rather than faith based. In practice, the fear of being caught and disgraced are often larger drivers in the West than humanisticvalues, which in Islam's shariah are the major force guiding governance.

Theory	Agency (Western)	Stewardship (Islamic)
Management and leadership act as	Agents	Stewards
Management/leadership's behavioral model is	Individualistic Opportunistic Self-serving	Collectivistic Pro-organizational Trustworthy
Management and leadership are motivated by	Their own objectives	Principal's objectives
Management/leadership's and principal's interests	Diverge	Converge

EXHIBIT 46.1 AGENCY AND STEWARDSHIP THEORY

Second, Western business concepts are rooted in self-interest with no compelling requirement to meet the larger interests of society. This may seem like a harsh assessment, but look to see the last time a rating agency downgraded a corporation for poor moral or unethical behavior. As the stock option scandal spreads in the United States with corporation after corporation restating earnings, the only downgrades come with reduced earnings, not from the flagrant lapses in ethical judgment.

Third, Western governance concepts are based on agency theory rather than stewardship theory, which is more in line with Islamic beliefs. Agency theory and stewardship theory are summarized in Exhibit 46.1.[2]

Islamic governance would be more likely to embrace a stewardship and partnership approach in which directors and executives act in the best interests of their principals and the overall well-being of the firm rather than as opportunistic and self-interested agents who require rigorous monitoring. Unlike the West, Islam does not accept the separation of the secular from the religious. There is no equivalent to the New Testament to render unto Caesar the secular and unto God the sacred and religious.[3]

The major distinctions between Western and Islamic approaches to governance can be found in the concepts of shariah, shura, and religious supervision and audit.

- *Shariah* is an Arabic word meaning the way to the source of life and is now being embraced as a legal code of behavior. Shariah includes a ban on usury in favor of a shared risks and rewards system. (This is discussed in much greater detail in our Islamic Finance chapter.)
- Islamic law also calls for a shuratic decision-making process to encourge consultation and participation in an open and frank discussion.
- Religious supervision and audit are required in Islam, because all resources are seen to be given by God and therefore accountable to God. Man is only a trustee of God-given resources, and the audit of corporate boards and executives is a means to inform shareholders and other stakeholders that the organization is acting in an acceptable manner.[4]

All Islamic business activity should follow concepts of oneness and unity of God, trust in God as evidenced by moderation, justice, kindness, honesting, patience, and spending to meet social obligations and public interests. There are also many negative activities to be avoided: hoarding of wealth, tyranny, miserliness, greed, and extravagance.[5]

46.2 ISLAMIC FINANCIAL INSTITUTIONS DRIVE IMPROVED CORPORATE GOVERNANCE

Islamic financial institutions can be viewed as leading the way for improved corporate governance in the Islamic world. This is the same trend in the largest nations, with the Basel II accords requiring much enhanced capital adequacy for large global banks. As with the leading economies, banking can be a good role model for nonfinancial institutions in improved transparency, operational risk, quantitative methods, and rewards for improved capital management.

Why banking? The reason is simple—that is where the money is. Financial institutions are typically the most heavily regulated institutions in any country, at least in terms of financial compliance. Islamic banks have become a major factor in creating wealth and underwriting global projects. The total value of these activities is now approaching $1 trillion.[6]

Islamic banks and related financial institutions are unique in applying Islamic religious principles, which are discussed in great detail in our Islamic Finance chapter. These principles include a strong moral foundation to corporate governance—that money is to be used to do good things and that agreements should never exploit any of the parties to the agreement.

While many Christians in the West preach a moral foundation to business, there is typically a weak connection in practice, as evidenced by a never ending series of scandals based on unabashed greed—usually by multimillionaires seeking even greater wealth. This is especially ironic in the United States, in which the great majority of citizens surveyed classify themselves as Christians.

Ironically, the United States took a bottom-up and rules-based approach to governance rather than the top-down approach one would expect in a strong Christian nation. This would mandate a strong tone at the top to drive improved governance, rather than a system of complex and ineffective rules that continue to be circumvented by very clever and very unethical senior executives. Nations that grew up under British influence took a stronger top-down approach that placed the burden on corporate boards to provide the needed moral and ethical character to drive governance. Canada, Australia, and the UK all enjoy high rates of governance based on this approach and without the huge costs associated with the American approach.

Islamic governance is faith-based, and, unlike the U.S. system, there is a strong bond between theory and practice. Like the British system, the burden is on the leadership of any organization to provide the moral and ethical character to drive compliance. Also like the British system, shariah principles advocate

leading by example. Shariah principles also stress maximizing shareholders' and stakeholders' wealth in a shared risk and shared awards approach. In practice, there are few hard-and-fast rules as to how shariah principles are applied, which is understandable given the cultural, ethnic, and geopolitical diversity of the Islamic world.

46.3 HARMONIZING WESTERN AND ISLAMIC GOVERNANCE

So the major question is whether Islamic faith-based governance is compatible with Western corporate governance. The short answer is yes. Muslim nations, like much of the rest of the world, are being driven to standardize and harmonize corporate governance and improve financial transparency in order to attract equity capital and expand global trade. The alternative is not very appealing—a subservient role in the global economy.

The biggest issue in harmonizing Western and Islamic notions of governance is the legal structure of corporations and their relationship with shareholders and regulators. Islamic law and the Qur'an predate the development of corporations. Therefore, there are challenges in extending Islamic laws to modern corporate structures. The failures of Western agency-based governance to protect stockholders and other stakeholders (employees, suppliers, customers, and communities) do give greater credance to the stewardship approach of a faith-based governance approach. Muslims do not feel comfortable with the hands-off nature of Western stock exchanges in which investors rarely care about the internal workings or social responsibilities of the companies in which they invest.

Muslims would typically reject the separation of corporate ownership and social responsibility. Stockholders have a responsibility to acquaint themselves about what is taking place in the organizations in which they invest. The fact that Western accounting relieves shareholders of any obligations beyond their personal investments in no way removes this obligation under Islamic law.

Harmonizing Islamic and Western governance could be accomplished by expanding financial reporting to capture areas important to Muslims, such as breaking out costs/expenditures and profits/income based on:

- Their categories: allowed, forbidden, permissible, reprehensible, and so on
- Support of basic necessities needed by Muslims
- Environmental impact of business activities

Another means of harmonizing Islamic and Western governance is to expand the stewardship resonsiblies of Western corporations. The UK's Combined Code, India's Clause 49, and Australia's ASX 10 principles are all examples of holding corporate boards to a much higher standard of stewardship and recognizing that corporations have a responsibility for doing good and ethical things, and not just in improving shareholder wealth.

On the Islamic side, there is a need to improve the six areas of governance tracked by the World Bank and detailed later in this chapter: control of

corruption, regulatory quality, the rule of law, voice and accountability, political stability/violence, and government effectiveness.

In an Islamic financial institution, a shariah advisor would be essential to guide Islamic corporate governance. The advisor would have to have a strong financial and religious foundation. Imagine a bank in which a morality advisor is given as much attention and credence as internal and external auditors looking to meet regulatory bodies' standards and accepted best practices. Now imagine that these goals are aligned—a convergence of shariah and Western governance principles. What better way to provide shareholders and stakeholders with confidence in an institution?

As with much of the world, achieving transparency may be the largest challenge. A primary object of shariah is to ensure greater transparency and accountability in order to provide fairness to shareholders and stakeholders. This would be achieved by examining the structure of transactions to determine if they invalidate potential gains or profits. Secular corporate governance follows a similar logic and methodology to assure compliance with corporate rules and regulations.[7]

46.4 CORPORATE GOVERNANCE IN LARGER MUSLIM NATIONS

In evaluating the status of corporate governance in Islamic nations, we decided to focus on nations with over 10 million Muslims and with a majority Muslim population. There are 24 nations with a Muslim population 10 million or more—the largest being Indonesia (196 million), India, and China (each with 133 million). Of these, 19 nations have both a majority Muslim population and over 10 million Muslims (see Exhibit 46.2). They represent:

- Fully 75 percent of the 1.3 billion Muslims in the world
- Some 7.6 percent of global gross national product (GDP) as measured by purchasing power parity (PPP)
- Three African, nine Middle East, and North Africa (MENA), and three South and Southeast Asia nations
- Three of the world's largest oil-producing nations—Saudi Arabia, Iran, and Iraq
- Two countries at war—Iraq and Afghanistan
- One country with nuclear weapons—Pakistan
- One NATO member—Turkey

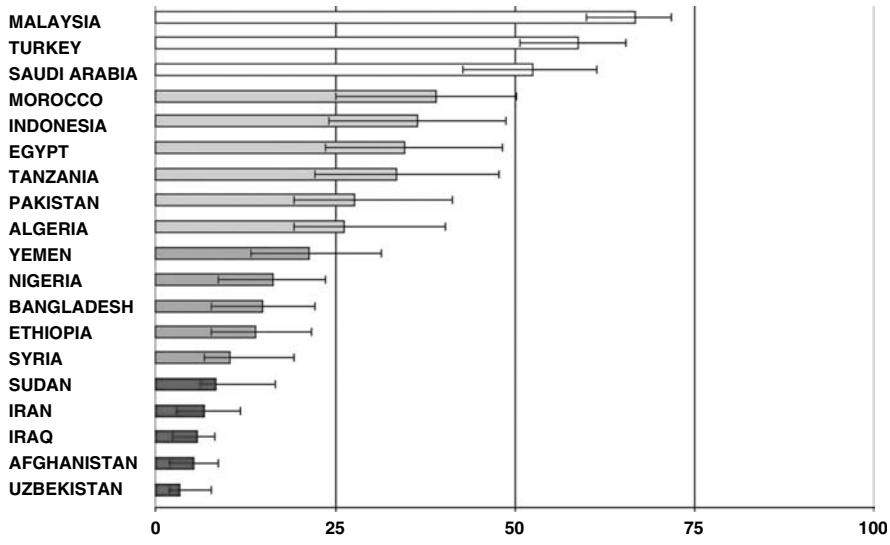
The World Bank publishes country-to-country and year-to-year evaluations covering six areas of governance. Exhibits 46.3 to 46.6 are examples of four World Bank governance elements. Malaysia, Turkey, and Saudi Arabia lead in most of these elements.

By taking an average of the World Bank's six governance elements, we can rank and grade each of the 19 Islamic nations against the top gross domestic product (GDP) nations worldwide. We applied a simple five-point grading system

Over 10 Million Muslims
Over 50 Percent of Total World Population Is Muslim

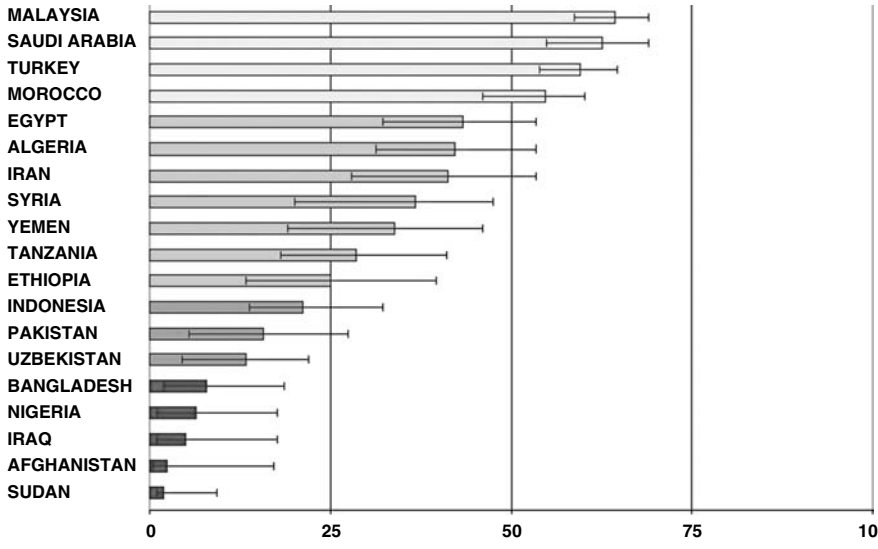
Nation	Majority Sect	Total Pop. (Millions)	Muslim Pop. (Millions)	% Muslims	GDP (PPP) $ Billions	Global GDP Rank
Afghanistan	Sunni	22.7	22.7	100%	$ 21.5	111
Algeria	Sunni	29.2	28.9	99%	$ 233.2	38
Bangladesh	Sunni	123.1	104.6	85%	$ 304.3	31
Egypt	Sunni	63.6	59.8	94%	$ 303.5	32
Ethiopia	Sunni	57.2	37.2	65%	$ 62.9	71
Indonesia	Sunni	206.6	196.3	95%	$ 865.6	15
Iran	Shiite	66.1	65.4	99%	$ 561.6	19
Iraq	Sunni	21.4	20.8	97%	$ 94.1	59
Malaysia	Sunni	20.0	10.4	52%	$ 290.2	33
Morocco	Sunni	29.8	29.4	99%	$ 138.3	55
Nigeria	Sunni	103.9	77.9	75%	$ 174.1	47
Pakistan	Sunni	129.3	125.4	97%	$ 393.4	26
Saudi Arabia	Sunni	19.4	19.4	100%	$ 338.0	28
Sudan	Sunni	31.5	26.8	85%	$ 85.7	61
Syria	Sunni	15.6	14.0	90%	$ 72.3	66
Tanzania	Sunni	29.1	18.9	65%	$ 27.1	101
Turkey	Sunni	62.5	62.4	99%	$ 572.0	18
Uzbekistan	Sunni	23.4	20.6	88%	$ 48.2	78
Yeman	Sunni	13.5	13.3	99%	$ 19.4	114

EXHIBIT 46.2 MUSLIM POPULATION



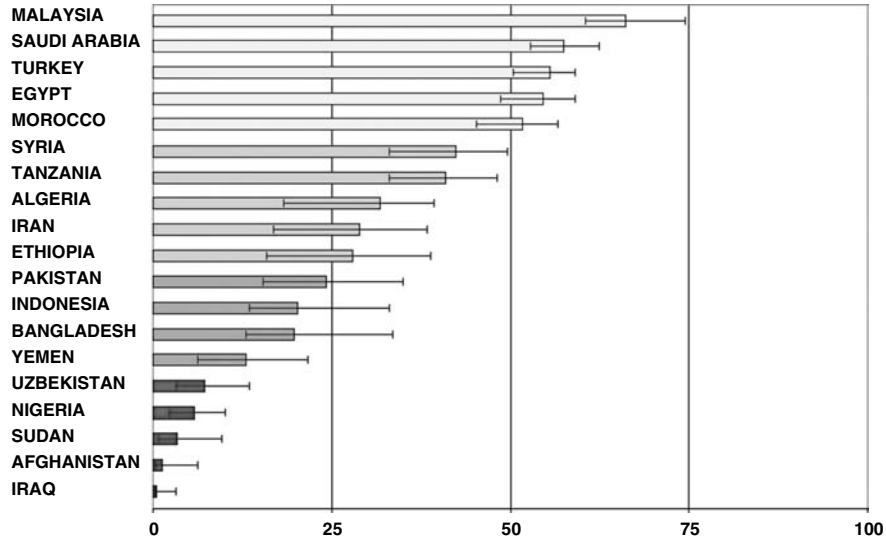
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (September 2006), Available at SSRN: http://ssrn.com/abstract=929549

EXHIBIT 46.3 WORLD BANK REGULATORY QUALITY: MAJOR ISLAMIC ECONOMIES



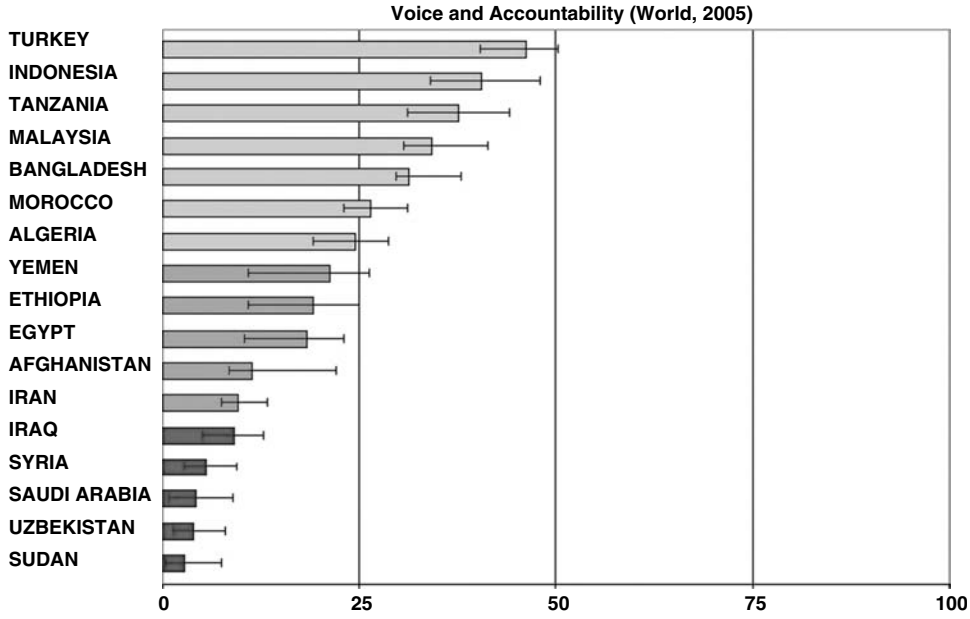
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (September 2006).

EXHIBIT 46.4 WORLD BANK CONTROL OF CORRUPTION: MAJOR ISLAMIC ECONOMIES



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (World Bank, September 2006).

EXHIBIT 46.5 WORLD BANK RULE OF LAW: MAJOR ISLAMIC ECONOMIES



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (World Bank, September 2006).

EXHIBIT 46.6 WORLD BANK VOICE AND ACCOUNTABILITY: MAJOR ISLAMIC ECONOMIES

with A = top 20 percent (excellent), B = next 20 percent (above average), C = next 20 percent (average), D = next 20 percent (below average), F = bottom 20 percent (failing). By these criteria, only Malaysia is performing above average. By comparison, the 16 nations in the top GDP worldwide achieved an above average grade. (See Exhibit 46.7 and Exhibit 46.8.)

46.5 THE RELATIONSHIP BETWEEN GOVERNANCE AND FREEDOM, LITERACY, AND WEALTH

We next wanted to look at the relationships between various factors and the World Bank governance rankings. As shown in Exhibit 46.9, we compared governance to:

- Per capita gross national product (GDP) as measured by purchasing power parity (PPP), which is preferred because it attempts to equalize purchasing power from one nation to the next
- Freedom as measured by political rights and civil liberties
- Literacy rates for men and women

Applying a 0 to 4 scale to the grades, it is possible to determine the correlation as measured by a standard deviation across the four categories. (See

Larger Islamic Nations	World Bank Governance Ratings							
	Six Element Grade	Six Element Average	Voice & Accountability	Political Stability	Gov't Effectiveness	Regulatory Quality	Rule of Law	Corruption Control
			Major Islamic Nations					
Afghanistan	**F**	**5.3%**	12%	2%	9%	5%	1%	3%
Algeria	**D**	**31.2%**	25%	18%	43%	27%	32%	42%
Bangladesh	**F**	**17.0%**	31%	7%	21%	15%	20%	8%
Egypt	**D**	**37.5%**	18%	21%	43%	35%	55%	53%
Ethiopia	**F**	**18.3%**	19%	8%	16%	14%	28%	25%
Indonesia	**D**	**27.5%**	41%	9%	37%	37%	20%	21%
Iran	**D–**	**21.5%**	10%	16%	26%	7%	29%	41%
Iraq	**F**	**3.7%**	9%	0%	1%	6%	1%	5%
Malaysia	**B–**	**62.3%**	34%	62%	80%	67%	66%	65%
Morocco	**C**	**42.2%**	27%	32%	48%	39%	52%	55%
Nigeria	**F**	**13.8%**	30%	5%	20%	16%	6%	6%
Pakistan	**D–**	**20.2%**	13%	6%	34%	28%	24%	16%
Saudi Arabia	**C–**	**41.0%**	4%	26%	42%	53%	58%	63%
Sudan	**F**	**4.5%**	3%	3%	8%	8%	3%	2%
Syria	**D–**	**20.8%**	6%	20%	9%	10%	43%	37%
Tanzania	**D**	**36.2%**	38%	33%	42%	34%	41%	29%
Turkey	**C**	**52.3%**	46%	30%	63%	59%	56%	60%
Uzbekistan	**F**	**6.8%**	4%	3%	10%	4%	7%	13%
Yemen	**F+**	**19.0%**	21%	7%	18%	21%	13%	34%
Averages	**D**	**25.3%**	21%	16%	30%	26%	29%	30%

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (World Bank, September 2006).

EXHIBIT 46.7 WORLD BANK GOVERNANCE RATINGS: MAJOR ISLAMIC ECONOMIES

Top 75% of Global GDP Nations								
Top GDP Nations	**Six Element Grade**	**Six Element Average**	**Voice & Accountability**	**Political Stability**	**Gov't Effectiveness**	**Regulatory Quality**	**Rute of Law**	**Corruption Control**
Australia	A	**90.8%**	90%	82%	92%	94%	96%	96%
Brazil	C	**50.1%**	57%	41%	55%	55%	43%	48%
Canada	A	**92.0%**	95%	79%	96%	95%	95%	94%
China	D	**36.6%**	6%	39%	52%	45%	41%	31%
France	A–	**82.2%**	92%	59%	90%	80%	90%	91%
Germany	A	**87.0%**	94%	67%	90%	90%	94%	94%
India	C	**45.3%**	56%	22%	52%	41%	56%	47%
Indonesia	D	**28.8%**	41%	9%	37%	37%	20%	21%
Italy	B	**68.5%**	77%	53%	72%	76%	64%	68%
Japan	A–	**83.0%**	75%	80%	85%	86%	89%	85%
Mexico	C	**50.0%**	54%	36%	57%	62%	40%	44%
Russia	D	**29.7%**	26%	19%	39%	44%	22%	28%
S. Korea	B	**70.4%**	68%	61%	79%	72%	73%	69%
Spain	A–	**81.9%**	87%	60%	90%	88%	85%	90%
UK	A	**86.8%**	93%	59%	94%	94%	93%	95%
US	A	**83.1%**	90%	49%	92%	93%	92%	92%
Averages	**B**	66.6%	69%	51%	73%	72%	68%	68%
Variance: Top Muslim Nations vs. Top 75% GDP Nations		**–41%**	**–48%**	**35%**	**–43%**	**–46%**	**–39%**	**–38%**

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, "Governance Matters V: Governance Indicators for 1996–2005" (World Bank, September 2006).

EXHIBIT 46.8 WORLD BANK GOVERNANCE RANKING TOP GDP ECONOMIES

	Per Capita GDP		Freedom				Literacy Rates			World Bank Governance	
			1 = Best 7 = Worst								
Nation	Per Capita GDP $	GDP Grade	Political Rights	Civil Liberties	Average	Freedom Grade	Male	Female	Literacy Grade	Six Element Average	Governance Grade
Afghanistan	$ 800	F	5	5	5.0	D	51%	21%	D	5.3%	F
Algeria	$ 110	F	6	5	5.5	D	70%	61%	B	31.2%	D
Bangladesh	$ 2,100	D	4	4	4.0	C	54%	32%	C–	17.0%	F
Egypt	$ 3,900	D	6	5	5.5	D	68%	47%	C+	37.5%	D
Ethiopia	$ 900	F	5	5	5.0	D	50%	35%	C–	18.3%	F
Indonesia	$ 3,600	D	2	3	2.5	B+	92%	83%	A	27.5%	D
Iran	$ 8,400	B–	6	6	6.0	D–	85%	73%	A–	21.5%	D–
Iraq	$ 1,800	F+	6	5	5.5	D	56%	24%	C–	3.7%	F
Malaysia	$ 12,000	B	4	4	4.0	C	92%	85%	A	62.3%	B–
Morocco	$ 4,100	D	2	1	1.5	A	64%	39%	C	42.2%	C
Nigeria	$ 1,400	F	4	4	4.0	C	26%	10%	F+	13.8%	F
Pakistan	$ 2,400	D	6	5	5.5	D	61%	35%	C	20.2%	D–
Saudi Arabia	$ 13,100	B	7	6	6.5	D–	85%	71%	B+	41.0%	C–
Sudan	$ 2,100	D	7	7	7.0	F	72%	51%	B+	4.5%	F
Syria	$ 3,900	D	7	7	7.0	F	89%	64%	B	20.8%	D–
Tanzania	$ 700	F	4	3	3.5	C+	86%	71%	B+	36.2%	D
Turkey	$ 8,400	B–	3	3	3.0	C+	94%	78%	A	52.3%	C
Uzbekistan	$ 1,900	D–	7	7	7.0	F	99%	99%	A	6.8%	F
yeman	$ 900	F	5	5	5.0	F	71%	31%	C	19.0%	F+
Islamic Average	**$ 3,816**	D	**5.1**	**4.7**	**4.9**	D	**72%**	**53%**	B–	**25%**	D
Top 75% GDP	**$ 21,223**	B	**1.9**	**2.1**	**2.0**	B	**95%**	**92%**	A	**67%**	B
World	**$ 9,501**	C	N/A	N/A	N/A	N/A	**87%**	**77%**	A–	N/A	N/A

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (World Bank, September 2006).

EXHIBIT 46.9 PER CAPITA GDP VERSUS FREEDOM VERSUS LITERACY RATES VERSUS WORLD BANK GOVERNANCE: INDIVIDUAL GRADES FOR MAJOR ISLAMIC ECONOMIES

Exhibit 46.10.) Typically standard deviations at or below 1.0 indicate a close correlation. In our sample, the 19 Muslim nations averaged a standard deviation of 1.2, indicating a fairly close correlation. The correlation for the top 75 percent GDP nations is even closer at 0.6, so it is logical to expect governance to improve in Muslim countries as per capita GDP, freedom, and literacy improve.[8]

A standard deviation is a statistic that indicates the amount of variability in a series of number or scores. When normally distributed (as part of a normal or bell-shaped curve), about two-thirds of the scores will be within one standard deviation of the average, or mean, score, and about 95 percent of scores are within two standard deviations of the mean. In almost any shaped distribution, all scores will be within five standard deviations of the mean score.

With a standard deviation of 1.2, there does appear to be a direct correlation between World Bank governance ratings and per capita income, freedom, and literacy. Eight nations have a correlation under 1.0, which indicates a strong correlation. Only Syria and Uzbekistan have a high negative correlation, and combined they represent only 3.5 percent of the Muslim population of larger Muslim nations. Removing these two nations, the standard deviation would be lowered to 1.0, indicating a high direct correlation.

46.6 THE RELATIONSHIP BETWEEN GOVERNANCE AND PER CAPITA GDP GROWTH

Next we examined the correlation between per capita GDP growth as measured by PPP and the World Bank governance rankings. (See Exhibit 46.11.)

Islamic nations are among the fastest growing economies in the world with an average growth rate of 6.2 percent, but have lower governance ratings. With a standard deviation of 1.5, there does not appear to be a direct correlation between high growth rates and good governance ratings. These are same conclusions we find for the top 75 percent of GDP nations. Specifically, China and India are growing very rapidly, but received low governance ratings. Conversely, several EU nations, Canada, Australia, and the United States, with very high governance ratings, received low growth ratings.

46.7 THE RELATIONSHIP BETWEEN GOVERNANCE AND TRADE

Next we examined the relationship between trade and governance. We took total trade (imports plus exports) as a percent of GDP as our criterion. (See Exhibit 46.12.)

Islamic nations typically do not have a high rate of trade as a percentage of their GDPs. They average 10 percent below global averages and 12 percent below the top GDP nations as measured by PPP. With a standard deviation of 0.6, there does appear to be a very strong direct correlation between governance scores and globalized trade. This makes sense and follows the argument that greater cross-border dealings and co-dependence require higher and more harmonized

Nation	Per Capita GDP		Freedom		Literary		World Bank Governance Six Elements		Overall Grade		Standard Deviation
Afghanistan	**F**	0.0	**D**	1.0	**D**	1.0	**F**	0.0	**0.5**	**D–**	**0.6**
Algeria	**F**	0.0	**D**	1.0	**B**	3.0	**D**	1.0	**1.3**	**D+**	**1.3**
Bangladesh	**D**	1.0	**C**	2.0	**C–**	2.5	**F**	0.0	**1.4**	**D+**	**1.1**
Egypt	**D**	1.0	**D**	1.0	**C+**	2.5	**D**	1.0	**1.4**	**D+**	**0.8**
Ethiopia	**F**	0.0	**D**	1.0	**C–**	1.5	**F**	0.0	**0.6**	**D–**	**0.8**
Indonesia	**D**	1.0	**B+**	3.5	**A**	4.0	**D**	1.0	**2.4**	**C**	**1.6**
Iran	**B–**	2.5	**D–**	0.5	**A–**	3.5	**D–**	0.5	**1.8**	**C–**	**1.5**
Iraq	**F+**	0.1	**D**	1.0	**C–**	2.5	**F**	0.0	**0.9**	**D**	**1.2**
Malaysia	**B**	3.0	**C**	2.0	**A**	4.0	**B–**	2.5	**2.9**	**B–**	**0.9**
Morocco	**D**	1.0	**A**	1.0	**C**	2.0	**C**	2.0	**1.5**	**C–**	**0.6**
Nigeria	**F**	0.0	**C**	2.0	**F+**	0.5	**F**	0.0	**0.6**	**D–**	**0.9**
Pakistan	**D**	1.0	**D**	1.0	**C**	2.0	**D–**	1.0	**1.3**	**D+**	**0.5**
Saudi Arabia	**B**	3.0	**D–**	0.5	**B+**	3.5	**C–**	1.5	**2.1**	**C**	**1.4**
Sudan	**D**	1.0	**F**	0.0	**B+**	3.5	**F**	0.0	**1.1**	**D**	**1.7**
Syria	**D**	4.0	**F**	0.0	**B**	3.0	**D–**	0.5	**1.9**	**C–**	**1.9**
Tanzania	**F**	4.0	**C+**	2.5	**B+**	3.5	**D**	1.0	**2.8**	**B–**	**1.3**
Turkey	**B–**	0.0	**C+**	2.5	**A**	4.0	**C**	2.0	**2.1**	**C**	**1.7**
Uzbekistan	**D–**	0.5	**F**	0.0	**A**	4.0	**F**	0.0	**1.1**	**D**	**1.9**
Yemen	**F**	0.0	**F**	0.0	**C**	2.0	**F+**	0.5	**0.6**	**D–**	**0.9**
Averages	**D**	**1.2**	**D**	**1.2**	**B–**	**2.8**	**D–**	**0.8**	**1.5**	**D+**	**1.2**

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (World Bank, September 2006).

EXHIBIT 46.10 PER CAPITA GDP, FREEDOM, LITERACY, GOVERNANCE: OVERALL GRADE AND STANDARD DEVIATIONS FOR MAJOR ISLAMIC ECONOMIES

Nation	Per Capita GDP Growth				World Bank Governance Six Elements		Standard Deviation
	Percent	Global Rank	Grade				
Afghanistan	8.4%	24	**A**	4.0	**F**	0.0	**2.8**
Algeria	5.6%	73	**B**	3.0	**D**	1.0	**1.4**
Bangladesh	6.1%	59	**B**	3.0	**F**	0.0	**2.1**
Egypt	5.7%	70	**B**	3.0	**D**	1.0	**1.4**
Ethiopia	8.5%	23	**A**	4.0	**F**	0.0	**2.8**
Indonesia	5.4%	82	**C**	2.0	**D**	1.0	**0.7**
Iran	5.0%	100	**C**	2.0	**D–**	0.5	**1.1**
Iraq	3.1%	156	**D**	1.0	**F**	0.0	**0.7**
Malaysia	5.5%	79	**C+**	2.8	**B–**	2.5	**0.2**
Morocco	6.7%	46	**B**	3.0	**C**	2.0	**0.7**
Nigeria	5.3%	84	**B**	3.0	**F**	0.0	**2.1**
Pakistan	6.5%	50	**B**	3.0	**D–**	1.0	**1.4**
Saudi Arabia	5.9%	66	**B**	3.0	**C–**	1.5	**1.1**
Sudan	9.6%	15	**A**	4.0	**F**	0.0	**2.8**
Syria	2.9%	167	**F**	0.0	**D–**	0.5	**0.4**
Tanzania	13.0%	5	**A**	4.0	**D**	1.0	**2.1**
Turkey	5.2%	89	**C**	2.0	**C**	2.0	**0.0**
Uzbekistan	6.8%	19	**A**	4.0	**F**	0.0	**2.8**
Yemen	3.2%	24	**A**	4.0	**F+**	0.5	**2.5**
Islamic Average	**6.2%**	**58**	**B–**	**2.9**	**D–**	**0.8**	**1.5**
Global Average	**5.1%**	**92**	**C**				

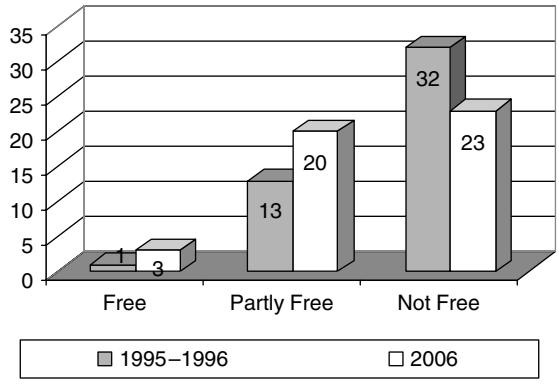
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (World Bank, September 2006).

EXHIBIT 46.11 PER CAPITA GDP GROWTH FOR MAJOR ISLAMIC ECONOMIES

Trade (Imports + Exports) as Percent of GDP (PPP)					World Bank Governance Six Elements		
Nation	**Percent**	**Global Rank**	**Grade**				**Standard Deviation**
Afghanistan	20.2%	174	**F**	0.0	**F**	0.0	**0.0**
Algeria	32.8%	138	**D**	1.0	**D**	1.0	**0.0**
Bangladesh	7.5%	211	**F**	0.0	**F**	0.0	**0.0**
Egypt	18.3%	177	**F**	0.0	**D**	1.0	**0.7**
Ethiopia	7.2%	213	**F**	0.0	**F**	0.0	**0.0**
Indonesia	19.3%	175	**F**	0.0	**D**	1.0	**0.7**
Iran	17.8%	183	**F**	0.0	**D–**	0.5	**0.4**
Iraq	56.3%	77	**B**	3.0	**F**	0.0	**2.1**
Malaysia	92.6%	37	**A**	4.0	**B–**	2.5	**1.1**
Morocco	22.4%	164	**F+**	0.05	**C**	2.0	**1.4**
Nigeria	44.6%	105	**C**	2.0	**F**	0.0	**1.4**
Pakistan	10.8%	205	**F**	0.0	**D–**	1.0	**0.7**
Saudi Arabia	71.8%	58	**B**	3.0	**C–**	1.5	**1.1**
Sudan	16.9%	189	**F**	0.0	**F**	0.0	**0.0**
Syria	18.1%	179	**F**	0.0	**D–**	0.5	**0.4**
Tanzania	17.1%	188	**F**	0.0	**D**	1.0	**0.7**
Turkey	32.4%	137	**D**	1.0	**C**	2.0	**0.7**
Uzbekistan	17.3%	186	**F**	0.0	**F**	0.0	**0.0**
Yemen	6.8%	191	**F**	0.0	**F+**	0.5	**0.4**
Islamic Average	**27.9%**	**152**	**D**	**0.7**	**D–**	**0.8**	**0.6**
Top GDP Nations	**39.3%**	**118**	**C–**				
Global Average	**37.7%**	**124**	**D+**				

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, "Governance Matters V: Governance Indicators for 1996–2005" (World Bank, September 2006).

EXHIBIT 46.12 TRADE AS PERCENT OF GDP (PPP) FOR MAJOR ISLAMIC ECONOMIES



Source: Freedom House Annual Global Survey of Political and Civil Liberties.

EXHIBIT 46.13 FREEDOM IN ISLAMIC-MAJORITY NATIONS

governance standards. These are the same conclusions we find for the top 75 percent of GDP nations with a standard deviation of 1.1 between trade and governance scores.

46.8 CONCLUSION

Our research indicates a direct relationship between increased freedom and improved corporate governance. There are some encouraging indicators in improvements in freedom over the past ten years as the number of partially free and free Muslim-majority nations continues to rise. (See Exhibit 46.13.)

Our evaluation also indicates that there is in addition a direct correlation between improved governance and per capita purchasing power and literacy. Improvements in these areas provide the opportunity to improve confidence in Islamic corporations and attract equity capital.

There is one other characteristic of Muslim nations that will support improved governance, and it is the fundamental Muslim belief that business and money are a means for doing good and honorable things. It provides a moral foundation that has been lacking in much of the business world. Without such a moral foundation, capitalism becomes pure greed and no amount of punitive rules and regulations will be likely to succeed.

To use an American term, it can be argued that Muslims put their money where their mouth is. The evidence of this can be seen in the rise in Islamic banking and financing (explained in detail in our Islamic Finance chapter). However, this is not to gloss over major issues facing the Islamic world in adopting Western notions of corporations and the accompanying notions of governance.

Notes

1. Mervyn K. Lewis, "Islamic Corporate Governance," International Association for Islamic Economics, *Review of Islamic Economics* 9, no. 1, 2005, 5–29.
2. Alfonso Vargas Sanchez, "Development of Corporate Governance Systems: Agency Theory versus Stewardship Theory in Welsh Agrarian Cooperative Societies," University of Huelva and CENTRA, Head of the Management and Marketing Department.
3. Lewis, "Islamic Corporate Governance."
4. Ibid.
5. Ibid.
6. Dr. Shamshad Akhtar, "Shariah Compliant Corporate Governance," keynote address delivered at Annual Corporate Governance Conference Dubai on November 27, 2006.
7. Ali A. Ibrahim, "Convergence of Corporate Governance and Islamic Financial Services Industry: Toward Islamic Financial Services Securities Market," Georgetown Law Graduate Paper Series, 2006.
8. Population, GDP, per capita GDP, GDP growth, and literacy source: *CIA Fact Book*, January 2007; political rights and civil liberties rights source: Freedom House's 2006 Global Survey.

CHAPTER 47

GLOBAL COMPLIANCE PROGRAMS IN LATIN AMERICA: MAJOR CHALLENGES AND LESSONS LEARNED

Pedro Fabiano

47.1 INTRODUCTION

This chapter focuses on the challenges of implementing international and U.S. corporate governance requirements in Latin America. To this end, it briefly describes the political, economic, and business climate of the region considering authoritative sources and the experience of the author. U.S. laws that have

extraterritorial scope and major international initiatives that apply to Latin America are also summarized. Finally, lessons learned from recent self-disclosure cases are included to better illustrate the significance of establishing good corporate compliance programs with a global perspective.

47.2 POLITICAL AND BUSINESS CLIMATE

Latin America has made enormous improvements over the past two decades in political development, with all countries but Cuba having regular free and fair elections for head of state.

While the region overall experienced a gross domestic product (GDP) decline of 0.6 percent in 2002 and only a modest growth rate of 1.5 percent in 2003, the region rebounded with an estimated growth rate of 5.9 percent in 2004, surpassing even the most optimistic predictions. Every country in the region, with the exception of Haiti, experienced positive economic growth, and even per capita income for the region as a whole increased by more than 4 percent for the year. Countries that had suffered the deepest recessions in recent years—Argentina, Uruguay, and Venezuela—all experienced significant economic growth in 2004. Growth continued in 2005 at a rate of 4.5 percent, with Argentina and Venezuela registering the strongest growth rates, and a growth rate of 4.6 percent is projected for the region in 2006.[1]

In spite of the democratic progress and economic growth, several nations face considerable challenges that could threaten political stability, including persistent poverty, violent guerrilla conflicts, autocratic leaders, drug trafficking, increasing crime, and the rise of radical populism in several Latin American countries. In most countries, weaknesses remain in the state's ability to deliver public services, ensure accountability and transparency, and advance the rule of law to control corruption.

(a) GOVERNANCE AND CORRUPTION. Extensive research shows that foreign investment is lower in countries perceived to be corrupt, which further thwarts their chance to prosper. When countries improve governance and reduce corruption, they obtain a "development dividend" that, according to the World Bank Institute, can include improved child mortality rates, higher per capita income, and greater literacy.

The World Bank research conducted on governance indicators supports the fact that realistic improvement in a nation's rule of law or control of corruption could result in a significant percent increase in per capita incomes in the long term.

(i) The World Bank Governance Indicators. The research study *Governance Matters V,* published by the World Bank in 2006, presents a set of estimates of six dimensions of governance covering 204 countries and territories for 2005. The governance indicators are drawn from 31 separate data sets maintained by 25 different organizations worldwide. The data consist of surveys of firms and individuals, as well as the assessments of commercial risk-rating agencies, nongovernmental organizations and think tanks, and multilateral aid agencies.

Governance is broadly defined by the World Bank as *the traditions and institutions by which authority in a country is exercised*. The individual measures of governance perceptions were assigned to six categories capturing key dimensions of governance.

1. *Voice and accountability:* the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and free media.
2. *Political stability and absence of violence:* perceptions of the likelihood that the government will not be destabilized or overthrown by unconstitutional or violent means, including domestic violence and terrorism.
3. *Government effectiveness:* the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies.
4. *Regulatory quality:* the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development.
5. *Rule of law:* the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, the police, and the courts, as well as the likelihood of crime and violence.
6. *Control of corruption:* the extent to which public power is kept from being exercised for private gain, including both petty and grand forms of corruption, as well as capture of the state by elites and private interests.

The World Bank study for 2005 in Exhibit 47.1 shows that the Latin America average indicators score very low in all the six governance indicators. Also, the lowest ratings are reflected in the political stability, rule of law, and control of corruption indicators.

Governance Indicator	Latin America Regional Average, Percentile (1–100)(*)	OECD Regional Average, Percentile (1–100)(*)
Voice and Accountability	52.3	91.3
Political Stability/No Violence	35.8	77.7
Government Effectiveness	43.4	88.0
Regulatory Quality	47.3	91.1
Rule of Law	37.4	89.6
Control of Corruption	41.2	90.5

*Higher values imply better Governance ratings. Percentile rank indicates the percentage of regions that rate below the selected region.

EXHIBIT 47.1 WORLD BANK GOVERNANCE INDICATORS 2005: SIX ELEMENTS OF GOVERNANCE FOR LATIN AMERICAN AND OECD AVERAGES

Governance Indicator	Chile Percentile Rank (0–100)	Latin America Regional Average, Percentile (0–100)	OECD Regional Average, Percentile (0–100)
Voice and Accountability	82.6	52.3	91.3
Political Stability/No Violence	75.9	35.8	77.7
Government Effectiveness	86.1	43.4	88.0
Regulatory Quality	90.6	47.3	91.1
Rule of Law	87.4	37.4	89.6
Control of Corruption	89.7	41.2	90.5

*Higher values imply better Governance ratings. Percentile rank indicates the percentage of countries worldwide that rate below the selected country.

EXHIBIT 47.2 WORLD BANK GOVERNANCE INDICATORS 2005—CHILE, LATIN AMERICA AND OECD AVERAGES

Notably, Chile is the only country in the region that shows high rankings, which are closer to those of the Organization for Economic Cooperation and Development (OECD) countries. (See Exhibit 47.2.)

Country	2006 Percentile Rank (0–100)
Argentina	35.7
Bolivia	20.5
Brazil	41.4
Chile	87.6
Colombia	29.5
Costa Rica	64.8
Dominican Republic	39.5
Ecuador	16.2
El Salvador	37.6
Guatemala	14.3
Honduras	21.4
Mexico	40.5
Nicaragua	25.7
Panama	51.4
Paraguay	18.1
Peru	26.2
Uruguay	61
Venezuela	5.7

*Higher values imply better Governance ratings. Percentile rank indicates the percentage of countries worldwide that rate below the selected country.
Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 47.3 WORLD BANK GOVERNANCE RANKINGS: RULE OF LAW FOR LATIN AMERICAN COUNTRIES

Country	2006 Percentile Rank (0–100)*
Argentina	40.8
Bolivia	31.1
Brazil	47.1
Chile	89.8
Colombia	51.9
Costa Rica	67.0
Dominican Republic	34.0
Ecuador	24.8
El Salvador	53.9
Guatemala	26.7
Honduras	22.3
Mexico	46.6
Nicaragua	23.8
Panama	49.5
Paraguay	13.6
Peru	45.1
Uruguay	75.2
Venezuela	12.6

*Higher values imply better Governance ratings. Percentile rank indicates the percentage of countries worldwide that rate below the selected country.
Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 47.4 WORLD BANK GOVERNANCE RANKINGS: CONTROL OF CORRUPTION FOR LATIN AMERICAN COUNTRIES

Exhibits 47.3 and 47.4 show that the four largest economies of the Region—Mexico, Brazil, Argentina, and Venezuela—have significant weaknesses in enforcing the laws and controlling corruption.

In general, data from the World Bank governance indicators for 2005 show that democratic accountability and clean government go hand in hand. Countries such as Chile, Portugal, and Canada all are vibrant democracies with very little corruption, while countries with voice and accountability challenges such as China and the Russian Federation or, more extremely, Zimbabwe and Equatorial Guinea tend to have much more corruption. The study also shows that more than a dozen emerging economies, including, for example, Slovenia, Chile, Botswana, and Estonia, score higher on rule of law and control of corruption than some industrialized countries, such as Greece and Italy. This can also be seen in other dimensions of governance.

(ii) Transparency International's Corruption Perceptions Index. Transparency International states that the correlation between corruption and poverty is again in evidence in the results for Latin America of the 2006 Corruption Perceptions Index (CPI). In countries such as Haiti, Ecuador, and Honduras, with highest levels of perceived corruption, corruption continues to be one of the biggest obstacles to effectively fight poverty.

The results again call attention to the need for greater efforts to strengthen democratic institutions and to install functioning systems of control and mutual accountability that ensure public resources are used effectively. While there are no winners in Latin America, the index shows substantially higher scores for countries with relatively strong democratic institutions, such as Chile, Costa Rica, and Uruguay.

Out of 28 Latin American countries in the 2006 CPI, the great majority (16 countries) score below 5, which indicates serious perceived levels of domestic corruption. More than a third (11 countries) score below 3, which indicates a perception of rampant corruption. These include Argentina, Bolivia, Ecuador, Guatemala, Haiti, Honduras, Nicaragua, Paraguay, and Venezuela. Favoritism and the abuse of discretionary power by leadership in these countries are prevalent, making public resources there subject to private interests.

47.3 APPLICATION OF U.S. LAWS IN LATIN AMERICA

Latin American capital markets have recently experienced a wave of mergers and acquisitions where ownership of the largest domestic companies has been transferred to foreign companies. Also, during the past 10 years many of the largest Latin American companies have been on the U.S. markets through the American depositary receipt (ADR) program, while domestic trading has contracted, presenting lower turnover ratios and a very low level of new equity issues.

Approximately 1,200 foreign companies are listed on U.S. exchanges. The New York Stock Exchange (NYSE) has 450 foreign issuers, NASDAQ has about 300, and the remaining foreign companies trade on over-the-counter exchanges. Latin America had 89 companies listed in the NYSE by the end of 2005. The majority of these companies were headquartered in Brazil (35 companies), Chile (18), Mexico (17), and Argentina (12). The extraterritorial scope of the U.S. laws related to governance and anticorruption are briefly discussed in the following paragraphs.

(a) THE FOREIGN CORRUPT PRACTICES ACT OF 1977 AND THE SARBANES-OXLEY ACT OF 2002. The recent changes to laws and regulations in the United States with respect to governance and fraud have had a considerable impact on foreign private issuers and also on subsidiaries of U.S.-registered entities. A combination of Sarbanes-Oxley (SOX)'s greater focus on internal corporate controls, the increased penalties for Foreign Corrupt Practices Act (FCPA) books and records violations in SOX, and a continued aggressive U.S. government policy to target international business bribery has resulted in a significant level of FCPA enforcement activity since 2002.

It is important to highlight that there is no general exemption from the U.S. federal securities laws for foreign private issuers. If their securities are offered or traded in the United States, they need to concern themselves with these laws.

The two key provisions of the FCPA are the accounting provisions, commonly referred to as the books and records provisions, and the antibribery

provisions. The FCPA requires companies whose securities are listed in the United States to meet its accounting provisions. These accounting provisions, which were designed to operate in tandem with the antibribery provisions of the FCPA, require corporations to make and keep books and records that accurately and fairly reflect the transactions of the corporation and to devise and maintain an adequate system of internal accounting controls.

The antibribery provisions of the FCPA make it unlawful for a U.S. person, and certain foreign issuers of securities, to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person. Since 1998, they also apply to foreign firms and persons who take part in any act in furtherance of such a corrupt payment while in the United States.

The accounting provisions of the FCPA receive less publicity but are much more likely to form the basis of a government proceeding against companies subject to the Act. The most common FCPA enforcement mechanism is a civil action by the Securities and Exchange Commission (SEC) under the accounting provisions and not a criminal charge by the Department of Justice (DOJ) or even a civil action by the SEC under the antibribery provision. A study conducted in 2003 found that of 604 enforcement actions brought by the SEC since the FCPA was enacted in 1977, only 7 percent related to foreign bribery. The SEC has, in fact, used the FCPA in several cases to prosecute wrongdoers who have not engaged in bribery of foreign officials, but whose actions technically violate the Act's accounting requirements, much like the federal government has used tax laws to prosecute organized crime figures whose *real* crimes cannot be proven.

The Sarbanes-Oxley Act (SOX) is considered as the most stringent corporate governance policy so far. The intention of the Act is to help restore public trust in business and corporate reporting. Since the passage of SOX in 2002, the accounting provisions have assumed even greater importance because officers now are required to certify the integrity of their companies' financial statements and assess the adequacy of internal controls. As a result, companies are more frequently uncovering accounting-provision violations in connection with internal SOX reviews and are self-reporting these violations to regulators in hopes of mitigating penalties for noncompliance.

Several SOX provisions have contributed to the increase in self-reported FCPA cases, but two in particular, Sections 302 and 404, have fundamentally changed the approach companies take in preventing, detecting, and responding to fraudulent accounting practices. Moreover, certifying officers have a strong incentive to prevent and detect fraud. Under SOX Section 906, a criminal provision closely related to Section 302, a manager who willfully certifies a periodic report filed with the SEC that omits the requirements of the accounting provisions of the FCPA faces criminal penalties of up to 20 years in prison and/or fines of up to $5 million.

(i) The Federal Sentencing Guidelines (FSG). An effective anticorruption compliance program will help companies to proactively protect themselves against FCPA violations. The Federal Sentencing Guidelines for Organizations, issued by the U.S. Sentencing Commission and applicable to criminal violations of all federal statutes such as the FCPA and SOX, require federal courts handing down criminal sanctions to take into account the existence or absence of effective corporate compliance programs. The presence of an effective compliance program can significantly reduce a company's sentence, while the absence of such a program can increase the sentence.

(b) THE INTERNATIONAL ANTICORRUPTION AND GOOD GOVERNANCE ACT (IAGGA). The purpose of the International Anticorruption and Good Governance Act of 2000 (IAGGA) is "to ensure that United States assistance programs promote good governance by assisting other countries to combat corruption throughout society and to improve transparency and accountability at all levels of government and throughout the private sector."

The IAGGA amended the Foreign Assistance Act of 1961, adding to the list of major goals for United States foreign development policy "the promotion of good governance through combating corruption and improving transparency and accountability." The law also authorizes the U.S. president to establish programs "that combat corruption, improve transparency and accountability, and promote other forms of good governance" in countries where the United States has either a significant economic interest or provides significant foreign assistance, and where problems of corruption are most persistent.

The IAGGA further requires the secretary of state, in consultation with the secretary of commerce and the administrator of the United States Agency for International Development (USAID), to prepare a report to Congress that surveys United States government (USG) diplomatic and programmatic anticorruption efforts, as well as host government efforts, in priority countries. The IAGGA fourth biennial report focuses on notable activities by the USG in 2004–2005, and its conclusions can be summarized:

- Corruption remains a worldwide problem, affecting vital American interests. While a number of countries continue to make important strides in creating transparent, accountable systems to prevent, detect, and prosecute corruption, the effort against corruption is a constant battle.
- Longstanding U.S. diplomatic efforts and innovative new approaches to counter corruption worldwide have succeeded in bringing global attention to this serious problem and increasing global cooperation to fight it.
- Since the last report submitted in April 2004, the USG has helped to advance significant multilateral anticorruption commitments, including, most notably, promoting acceptance and implementation of UNCAC and also the "no safe haven" policy. Addressing kleptocracy and strengthening

cooperation on recovery of illicitly acquired assets by corrupt officials remains a critical area of focus for the USG.

- In addition, the United States continues to promote new anticorruption commitments and enhanced implementation efforts in multilateral processes such as the Inter-American Convention and Special Summit of the Americas, Council of Europe conventions, Stability Pact Anticorruption Initiative, the Asia-Pacific Economic Cooperation (APEC) Anticorruption and Transparency (ACT) Initiative, and the United Nations Development Program (UNDP)-Organization of Economic Cooperation and Development (OECD) for Middle East and North Africa (MENA) Initiative and at the OECD. The United States will also explore new ways on engaging governments in Africa to strengthen their capacity to fight corruption.
- The United States continued its high-level participation in this effort, including sending a senior delegation to Brazil in 2005, and planning a similar effort for the next Global Forum in South Africa in 2007. The USG has focused attention and resources on promoting implementation of recommendations of mutual evaluation mechanisms and helping to develop effective governmental approaches to preventing corruption, providing U.S. experts and assistance to help over 60 countries implement anticorruption commitments.
- The United States has developed and funded innovative technical assistance programs that help to build the popular will against corruption and promote integrity within the private sector. The USG continues to enforce vigorously the Foreign Corrupt Practices Act (FCPA), to ensure robust implementation of the OECD Antibribery Convention, and to work with the U.S. private sector to ensure that businesses operating abroad understand their responsibilities under the FCPA, including intolerance for corruption in transnational business transactions.
- The United States also supports the efforts of the international financial institutions (IFIs) as they work to strengthen the operations of the internal investigative function in each institution to combat corruption, to help recipient countries improve governance and transparency in their public institutions, and to combat corruption in development project financing. Actions such as those taken by the World Bank to freeze loans to corrupt governments and pursue prosecution where contractors have engaged in corrupt practices send the important message that development dollars should be safeguarded and used productively. The USG is also exploring ways to engage the IFIs on kleptocracy and related anticorruption issues, including the return of illicitly acquired assets.
- With the leadership of the United States and other dedicated parties, the international fight against corruption will continue to move forward. The United States is committed to working to ensure that, 15 years from now,

taking effective actions against corruption becomes second nature for most governments in the world.

47.4 INTERNATIONAL INITIATIVES

(a) THE OECD CONVENTION AND THE REVISED RECOMMENDATION ON COMBATING BRIBERY OF FOREIGN PUBLIC OFFICIALS IN INTERNATIONAL BUSINESS TRANSACTIONS. The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, established by the governments of developed countries, is regarded as one of the most important instruments in the fight against corruption.

On November 21, 1997, the 29 member nations of the OECD and five nonmember nations adopted the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The OECD Convention, which was signed on December 17, 1997, and ratified by the U.S. Senate on July 1, 1998, sets forth the essential elements of a foreign corrupt practices statute that each signatory country is obligated to enact into law. All signatories to the convention also agreed to implement the Revised Recommendation that includes the elimination of the tax deductibility of bribes.

As of July 2003, all of the Convention's 35 signatories had laws on their books making it a crime to bribe a foreign public official. Mexico is the only Latin American country of the 30 current member states of the OECD. In addition, Argentina, Brazil, and Chile are signatories (but not members) of the Convention.

The Convention obligates the parties to criminalize bribery of foreign public officials in the conduct of international business. It proscribes the activities of those who offer, promise, or pay a bribe. For this reason, the Antibribery Convention is often characterized as a supply-side agreement, as it seeks to affect the conduct of companies in exporting nations.

The OECD Convention is relatively narrow and specific in its scope. Its sole focus is the use of domestic law to criminalize the bribery of foreign public officials. It focuses on active bribery, meaning the offense committed by the person who promises or gives the bribe, as contrasted with passive bribery, the offense committed by the official who receives the bribe. It does not apply to forms of corruption other than bribery, to bribery that is purely domestic, or to bribery in which the direct, indirect, or intended recipient of the benefit is not a public official. It also does not include cases where the bribe was paid for purposes unrelated to the conduct of international business and the gaining or retaining of some undue advantage in such business.

In the last Department of Commerce annual report to Congress under the International Anti-Bribery and Fair Competition Act of 1998, it is estimated that between May 1, 2003 and April 30, 2004, the competition for 47 contracts worth U.S. $18 billion may have been affected by bribery by foreign firms or foreign officials. Firms alleged to have offered such bribes won approximately 90 percent of the contracts in the deals for which information is available as to

their outcomes. The report also states that, although the overall bribery activity by OECD firms dropped substantially from the reporting years prior to 2002, firms from a few OECD countries continue to be involved in a disproportionate share of those allegations. Prior reports indicated that bribery allegations were related to contracts in multiple sectors, including energy, telecommunications, construction, transportation, and (primarily) military procurement.

(i) Inter-American Convention Against Corruption. The Inter-American Convention was negotiated under the auspices of the Organization of American States (OAS) following a mandate agreed to by the 34 heads of state that participated in the Summit of the Americas in 1994. The Inter-American Convention was adopted and opened for signature on March 29, 1996, in Caracas, Venezuela. Thirty-three of the 34 OAS member countries have now ratified.

The Inter-American Convention identifies acts of corruption to which the Convention will apply and contains articles that create binding obligations under international law as well as exhortatory principles to fight corruption. The Inter-American Convention also provides for institutional development and enforcement of anticorruption measures, requirements for the criminalization of specified acts of corruption and articles on extradition, seizure of assets, mutual legal assistance, and technical assistance where acts of corruption occur or have effect in one of the parties. In addition, subject to each party's constitution and the fundamental principles of its legal system, the Inter-American Convention requires parties to criminalize bribery of domestic and foreign government officials and illicit enrichment. The Inter-American Convention also contains a series of preventive measures that the parties agree to consider establishing to prevent corruption including systems of government procurement that assure the openness, equity, and efficiency of such systems and prohibiting the tax deductibility of bribes.

A monitoring mechanism for the Inter-American Convention was established in 2001, which assesses the progress made by parties in implementing their obligations of the Inter-American Convention. The U.S. State Department has produced annual reports to Congress monitoring the Inter-American Convention. According to the April 2004 report, Brazil, Nicaragua, and Suriname obtained convictions of officials for corruption. Chile, Mexico, Nicaragua, Paraguay, and Peru punished or removed high-level officials. Supreme Court justices were impeached in Argentina and Paraguay. Brazil, the Dominican Republic, Ecuador, Honduras, Jamaica, and Nicaragua brought corruption charges against high-level officials. The Bahamas, Costa Rica, Guatemala, and Paraguay brought investigations into high-level official corruption, and Mexico fined a political party for campaign financing violations.

(ii) United Nations Convention Against Corruption (UNCAC). The UN Convention Against Corruption is the first legally binding multilateral treaty to address on a global basis the problems relating to corruption. It makes the prohibition of corruption an integral part of the international public order.

Since the UNCAC opened for signature in December 2003, 140 nations have signed it and 80 have ratified it. The convention entered into force on December 14, 2005, for those countries that have ratified it.

The instrument provides a comprehensive framework for dealing with corruption in the public sector and in the private sector—this is particularly important for countries not covered by regional conventions. The Convention provisions include, among other things:

- It expands on the provisions of existing regional anticorruption instruments to prevent corruption and provides channels for governments to recover assets that have been illicitly acquired by corrupt former officials.
- It provides for the criminalization of certain corruption-related activities such as bribery and money laundering, and for the provision of mutual legal assistance related to those activities.
- It requires parties to institute a comprehensive domestic regulatory and supervisory regime for banks and financial institutions to deter and detect money laundering.
- That regime must emphasize requirements for customer identification, record keeping, and reporting of suspicious transactions.
- It prohibits the extortion by public officials and complements the OECD Convention's efforts to prohibit companies from bribing foreign officials.
- It addresses serious shortcomings in mutual legal assistance and asset recovery, two key tools for combating international corruption that can only be strengthened through comprehensive worldwide efforts.

In Latin America, 23 countries have signed the UNCAC and 16 have ratified it as of November 15, 2006. The six countries that have not yet ratified the convention are Barbados, Costa Rica, Haiti, Jamaica, Uruguay, and Venezuela.

47.5 LESSONS LEARNED FROM CASE STUDIES

In addition to FCPA enforcement in the United States, companies are increasingly facing parallel investigations in foreign jurisdictions under other nations' anticorruption laws. The FCPA is part of a broader international agenda to combat bribery that includes the Organization of American States' Inter-American Convention Against Corruption, the Organization for Economic Cooperation and Development's Convention on Combating Bribery of Foreign Officials in International Business Transactions, the United Nations' Convention Against Corruption, and policies instituted by the World Bank and the International Monetary Fund allowing for the investigation of corruption committed by companies and governments.

While the level of coordination between various governments and agencies currently conducting investigations is not fully apparent, the investigative and prosecutorial demands presented by these alleged violations are significant opportunities for the creation of an international standard of business propriety,

casting aside any doubts about the strength of the international anticorruption effort.

Importantly, the fight against fraud and corruption needs to be conducted on a broad front and to draw on support from a wide variety of actors, especially the business community. The business community's importance derives from the fact that it is on the front lines in the fight against corrupt business practices. Businesses' management practices determine whether companies will actually be able to comply with the evolving global legal framework and with growing societal pressures.

The development of comprehensive compliance programs to implement best practices in corporate governance, as part of the company standard business practice, may limit the company risk and help avoid potential costs of fraud and corruption. These programs can also help to protect the company's reputation, minimize its liability, and maintain its long-term viability.

The practices of self-disclosure and internal investigations are considered an integral part of a good compliance program. The following ten cases, obtained from SEC/DOJ filings, illustrate the significance of these practices in Latin America.

(a) CASE STUDY #1. Apex Silver Mines Limited is a Cayman Islands–based business engaged in the exploration and development of silver and other mineral properties in Latin America. Apex disclosed in March 2006 that it had concluded an internal investigation regarding payments made by employees of one of its South American subsidiaries to government officials that may have violated the FCPA. Apex also disclosed that the SEC had commenced an investigation of the matter. Apex reported in an SEC filing dated August 2006 that it is cooperating fully with the SEC investigation.

(b) CASE STUDY #2. Pride International Inc., a U.S. corporation, is an international provider of drilling services to oil and natural gas exploration and production companies. On August 2, 2006, Pride International disclosed in a Form 10-Q filing that an ongoing internal investigation found evidence suggesting that payments that might violate the FCPA were made from early 2003 through 2005 to government officials in Latin America, totaling less than $1 million. The company stated that the evidence to date suggests that the payments primarily were made either directly to government officials or to vendors serving as intermediaries in Venezuela and Mexico. The company stated that it believes it likely that members of its senior operations management either were aware or should have been aware of such improper payments and have placed such individuals on administrative leave pending the outcome of the investigation. The company voluntarily disclosed information relating to the allegations to the DOJ and SEC and is cooperating with those authorities.

(c) CASE STUDY #3. Sitel Corporation, a U.S. corporation, designs, builds, and operates customer service centers for companies around the world. Sitel

has disclosed that on March 1, 2006, it notified the SEC that it had identified accounting and other irregularities in its Brazil subsidiary that may have violated the FCPA. The irregularities involved accounting errors and a failure to remit municipal taxes. The company has stated that its investigation does not reveal any prior involvement or knowledge of the irregularities by any officer or director of Sitel and that the company is currently taking remedial actions.

(d) CASE STUDY #4. Horizon Offshore, Inc., a U.S. corporation traded on the NASDAQ, provides marine construction services for the offshore oil and gas industry, including installation, repair, and abandonment of marine pipelines and production platforms. On May 3, 2006, Horizon announced that as a result of an internal review, the company became aware of the possibility that one of its subsidiaries authorized an improper payment to a customs official in a Latin American country of approximately $35,000 in connection with the importation of construction equipment. The Audit Committee of Horizon's board of directors has engaged outside counsel to conduct an investigation of the allegations and of Horizon's internal controls, and has instituted disciplinary actions against several employees. The company has also notified and is fully cooperating with the SEC.

(e) CASE STUDY #5. Willbros Group, Inc. provides construction and engineering services to industry and government entities worldwide in oil, gas, and power sectors, specializing in pipelines and associated facilities in onshore, coastal, and offshore locations. Willbros International, Inc. (WII) is a wholly owned subsidiary of Willbros. In January 2005, Willbros announced that it had commenced an internal investigation relating to potential violations of the FCPA by the former president of WII, James Tillery. The company voluntarily disclosed its internal investigation to the SEC and DOJ, both of which launched investigations as well. The investigation determined that Tillery and others had violated the FCPA and other U.S. and international laws by making or approving improper payments to government officials in Bolivia, Nigeria, and Ecuador in exchange for construction contracts. Tillery resigned on January 6, 2005, following a preliminary investigation into a tax matter in Bolivia. The investigation revealed that Tillery and some 12 other employees and consultants appear to have owned interests in enterprises with whom WII did business, paying and receiving improper payments, corporate opportunities, and benefits from suppliers.

As of a June 2006 SEC filing, the company reported to be cooperating fully with the DOJ and SEC in their ongoing investigations. In an August 2006 SEC filing, Willbros announced an agreement in principle to settle consolidated class actions filed against it alleging, inter alia, that the conduct under investigation by the DOJ and SEC for potential FCPA violations also violated the Securities Exchange Act of 1934.

(f) CASE STUDY #6. ABB, Ltd., a Swiss corporation, is an energy and automation technologies company with operations in 100 countries. In April 2005, ABB

voluntarily disclosed to the SEC and DOJ that a potential violation of the FCPA might have been made by some of its employees in connection with ABB's software control business in the Middle East and Latin America. This disclosure stated that evidence of possible violations surfaced first during an internal investigation by ABB. This internal investigation had been initiated following a previous SEC inquiry into ABB's activities in Nigeria, Kazakhstan, and Angola. The new violations were discovered following an investigation of the dismissal of two managers from the company in 2004. In connection to this investigation, ABB became aware of suspect payments totaling $560,000 made to intermediaries in Latin America and the Middle East. ABB announced in February 2006 that it had disclosed to the DOJ and SEC the existence of additional suspect payments made by employees of company subsidiaries in a number of countries, including a country in the Middle East. According to the company's statement, ABB is continuing its investigation. ABB states that it is cooperating fully with the relevant authorities regarding these disclosures and is continuing international investigations. It is not yet known if the SEC or DOJ has launched separate formal investigations into these new alleged violations. In addition, ABB also stated in its January 2006 filing that, as part of the United Nations Independent Inquiry Committee investigation of the United Nations Oil-for-Food Program, certain ABB subsidiaries are alleged to have made illicit payments to the Iraqi government under contracts for humanitarian goods.

(g) CASE STUDY #7. AES Corporation, a U.S. corporation, is a global power company. The Government of the Dominican Republic filed a lawsuit against AES and three of its subsidiaries on March 23, 2006, in the United States District Court for the Eastern District of Virginia, claiming that AES violated, conspired to violate, and/or aided and abetted violation of the Foreign Corrupt Practices Act (FCPA), Racketeer Influenced and Corrupt Organizations Act (RICO), the Alien Tort Statute, and various other laws. The lawsuit alleges that, through its subsidiaries, AES illegally dumped more than 57,000 tons of coal ash waste in the Dominican Republic. The case is currently pending.

(h) CASE STUDY #8. DaimlerChrysler AG, a German corporation and manufacturer of automobiles, disclosed in an October 2004 SEC filing that the company was the subject of an SEC investigation into potential violations of the FCPA. The investigation followed a Department of Labor whistle-blower complaint filed by a former employee who was terminated earlier in the year. In November 2004, the Department of Labor dismissed the complaint, finding no reasonable cause to believe that the employee was terminated in violation of the Sarbanes-Oxley Act. Subsequent to the commencement of the investigation, the same employee filed a federal complaint in the United States District Court for the Eastern District of Michigan, alleging identical claims as the Department of Labor suit and additional federal and state law claims in connection with the termination. According to the complaint filed by the employee in federal district court, DaimlerChrysler AG maintained secret South American bank accounts that were used to bribe

foreign officials. The company is cooperating with the SEC. The employee, David Bazzetta, was subsequently fired from the company. In April 2005, the company reported it had undertaken its own internal investigation and had identified certain bank accounts that are receiving special scrutiny and had voluntarily shared this information with the SEC. The internal investigation conducted by the company is ongoing. In a March 2006 SEC filing, the company announced that improper payments were made in a number of jurisdictions, primarily in Africa, Asia, and Eastern Europe, raising concerns under the FCPA as well as German law and the laws of other jurisdictions. The company has taken a number of remedial actions, including termination of several employees, review and strengthening of internal controls, and establishment of a global compliance organization. The *Wall Street Journal* reported on September 14, 2006, that DaimlerChrysler AG is in talks with authorities at the DOJ and SEC to settle the allegations. The newspaper reported that the potential settlement was expected to involve payment of a financial penalty and that the parties had already agreed on the appointment of a monitor.

(i) CASE STUDY #9. Gtech Holdings Corp., based in West Greenwich, R.I., provides computer programming and data processing services. In an SEC filing in May 2004, Gtech disclosed that the SEC had begun an investigation into allegations that Gtech's former president and marketing director of Gtech Brazil offered an inducement in connection with the negotiation of an extension of Gtech's contract with Brazil's official lottery contractor. Gtech secured a contract extension in 2003, from which Gtech allegedly earned $650 million in revenue. At the time of this filing, the SEC announced an informal inquiry into the bribery allegations, with which Gtech cooperated. At some point in 2004, the SEC inquiry was upgraded to a formal investigation. The company is continuing to cooperate. Similar criminal and civil actions have commenced in Brazil. According to Gtech, in late March 2004, Brazilian prosecutor's recommended criminal charges be brought against nine individuals, including senior officers and the former president of Gtech Brazil, Antonio Carlos Rocha. In December 2004, the presiding judge rejected the prosecution's request to charge the individuals on procedural grounds. In January 2005, the prosecution reopened the investigation.

(j) CASE STUDY #10. In April 2006, the SEC instituted cease and desist proceedings against Oil States International, Inc. (OSI) for violations of the books and records and internal controls provisions of the FCPA, arising from certain payments made through its HWC subsidiary. The SEC stated that OSI, through certain employees of HWC, provided approximately $348,350 in improper payments to employees of Petroleos de Venezuela, S.A., an energy company owned by the government of Venezuela.

Notes

1. CIA Fact Book, December 2006 https://www.cia.gov/cia/publications/factbook/geos/id.html.

CHAPTER 48

SOUTHEAST ASIA CORPORATE GOVERNANCE

Lawrence Wasserman, PhD

48.1 BACKGROUND

For the past 15 years, Asia has served as the most dynamic region of the world with its impressive economic growth rates and development. Asia is now and for the near-term future the dynamic business engine of the first part of the twenty-first century.

This is in contrast to only 15 years ago when the East Asian economic crisis (in early 1990s) was the most important economic event in the region. The Asian

countries have seen a return to economic viability with trade and development, maturity, and political stability. However, there are countries where economic and private sector development remains stagnant.[1]

Political and worldwide trade negotiations in the 1990s saw Asian countries democratize their institutions and the lifting of social and trade barriers as advanced by the World Trade Organization (such as Generally Accepted Accounting Principles or GAAP).

Worldwide open trade movements prepared governments to introduce a system of free markets among the world countries, which had significant impact on the region's economy. Asian countries sought private sector investment and a movement to expand companies from social and control rule to a climate of entrepreneurship that has enhanced national wealth after years of regional stagnation.

In late 1990s a crisis arose in the United States at the corporate level (Enron, WorldCom, etc.) that then expanded to other worldwide markets of the global financial system, calling for a combination of financial deregulation and control, as well as removal of secrecy of events and activities within companies. The word *openness* became a common word in the financial industry for all parties: stakeholders, investors, boards of directors, and company managers.

The technological revolution resulted in an increase of interconnection of global markets and speed of transactions through computer technology and the development of large institutional financial players. As previously noted, the need to regulate the global financial system was identified as a result of the Asian crisis, and recommended by those who studied the collapse of markets.

Developing countries saw the impact of threats of volatile and large short-term capital flows that affected the economic stability of national market conditions. There was recognition on the need for greater transparency of how the global financial players and markets operate, and reforms at both international and national levels to regulate these speculative flows.

Transparency is now specifically needed among major institutions with regard to the ownership of financial assets, their behavior and operational methods, and the markets they operate in. The need for reform resulted from awareness by all shareholders, investors, and government regulators that the system is in the interests of financial owners and speculators.

Asia's financial crisis in 1997 underscored the importance of the need for structure and institutional reforms in the governance of the regional business sector. Initiatives to prevent future crises were begun and undertaken, both regionally and globally, in promoting corporate governance reform that became necessary for all governments to act upon.

Corporate governance initiatives in the Asia region resulted from Asia-Pacific Economic Commission (APEC) ministers' endorsement of the Pacific Economic Cooperation Council (PECC). PECC guidelines are for good corporate governance practices in 2001 and are revisited periodically.

PECC's assessment of corporate governance in Asian economies in 2005 measured the progress of corporate governance reforms in selected countries to be discussed. The study was based on the five corporate government principles revised in 2004 by the Organization for Economic Cooperation and Development (OECD). These principles are an extension of the OECD Principles of Corporate Governance endorsed by OECD ministers in 1999 and are an international benchmark for policy makers, investors, corporations, and other stakeholders worldwide.

The increased public awareness of financial and corporate scandals and problems resulting from corporate misdeeds resulted in the need for effective corporate governance.

Worldwide and Asian institutions and governments now had the opportunity to take decisive action on corruption, for if they didn't then the investment market could be severely damaged. Stockholder protection and the need for full disclosure and transparency must be established.

The United States passed the Sarbanes-Oxley Act of 2002, which is legislation in establishing principles guiding corporate enterprises. Known as the Public Company Accounting Reform and Investor Protection Act, this law was passed in response to a number of major corporate and accounting scandals, including those affecting Enron, Tyco, and WorldCom. These scandals resulted in a decline of public trust in accounting and reporting practices. In short, this legislation establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms.

In Europe the OECD established corporate governance requirements and updated them in 2004.[2] They are:

1. Ensuring the Basis for an Effective Corporate Governance Framework
2. The Rights of Shareholders and Key Ownership Functions
3. The Equitable Treatment of Shareholders
4. The Role of Stakeholders in Corporate Governance
5. Disclosure and Transparency
6. The Responsibilities of the Board

The Financial Stability Forum of OECD designated the Principles as one of the 12 key standards for sound financial systems. The Principles also provide the basis for an extensive program of cooperation between OECD and non-OECD countries and underpin the corporate governance component of World Bank/IMF Reports on the Observance of Standards and Codes (ROSC), which includes tracking corporate governance in Asian countries.

The World Bank and the Asian Development Bank proceeded to assist governments in developing and implementing laws to strengthen the financial and economic stability of countries and international cooperation on the need for development of corporate guidelines for financial institutions. In Asia, Singapore, and Hong Kong organizations established public, private, and educational institutions to conduct surveys and issued research reports on findings.

A timely review of the literature produced by institutions, associations, and university research organizations shows a robust level of assessment of national progress toward corporate governance. Conducted surveys, questionnaires, and assessments by public and private institutions illustrate progress in two ways. The first is a stocktaking, which took note of ongoing reforms in corporate governance rules and regulations Asia. The second covers attitudes, perceptions of the implementation, and enforcement of corporate governance rules as seen by surveys conducted of fund managers, shareholders, company officers, and analysts.

This chapter describes findings from several sources that provide the reader with an assessment of how selected Asian countries deal with the practice of regulation and compliance among private sector companies. The focus of public and private reports is on (1) the role and treatment of shareholders and stakeholders, (2) disclosure and transparency, and (3) board responsibilities.

Southeast Asia is a large geographic area, and those countries targeted in this report include Singapore, Malaysia, Vietnam, the Philippines, and Thailand. A cautionary note: Not all the countries are covered by each report or survey, and other sources of information have been utilized.

48.2 ASSESSMENT OF THE ASIA CORPORATE GOVERNANCE REGULATORY AND COMPLIANCE PROGRAM[3]

(a) LEGAL ENVIRONMENT. This section provides an overview on the legal aspects of Asian countries with respect to corporate governance from the perspective of public and private sector reports.

***(i) Asia-Pacific Economic Commission (APEC) Report*[4].** The Finance Forum Task Force on Macroeconomic Corporate Governance Scorecard of Pacific Economic Cooperation Council issued a report where APEC ministers endorsed the PECC guidelines (2001) for good corporate governance practices. The guidelines promoted governance practice in domestic corporations so that they could attract more investment from the international investment community.

This project focused on measuring the progress of corporate governance reforms in selected East Asian economies. The first survey assessed the progress ("stock-taking exercise") of ongoing reforms in present corporate governance rules and regulations, and the second reviewed the perceptions of the implementation and enforcement of corporate governance rules as seen by fund managers and analysts.

The survey was based on the five corporate governance principles developed by the OECD. These are the rights of shareholders, equitable treatment of shareholders, role of stakeholders, disclosure and transparency, and board responsibilities. The questionnaire was based on authors' selected questions relevant to these economies with added questions, and the survey was conducted during 2005.

The APEC report focused on applying several corporate governance indexes developed by the international investment community. For example, Standard & Poor's Transparency and Disclosure Index assessed the transparency and disclosure practices of corporations around the world. The Credit Lyonnais Corporate Governance Index applied some major corporate governance factors to rate corporations in different markets. These criteria include discipline, transparency, independence, accountability, responsibility, fairness, and social awareness.

The two surveys[5] yielded different results, showing that there is a deviation between the regulatory environment and market perception of corporate governance practices in these economies.

Key results from the surveys are:

- Economies equipped with the best rules and regulations are perceived to be the worst in terms of practice by investors. The results show that there is no significant difference in the rules and regulations among these economies, but that there is a significant difference in terms of market perception of their corporate governance practices.
- There are differences among Asian economies, and the pace of corporate governance reform in the region is at variance with each other. Performance of individual economies should be interpreted with great caution as it relates to their corporate governance.
- Good corporate governance enhances the well-being of the corporate sector but requires a vigilant board of directors, timely and adequate disclosure of financial information, meaningful disclosure about the corporation, and a transparent ownership.
- Corporate reforms are important and critical for corporations that want to raise funds from the international capital markets and are necessary to promote a viable company.

The survey questions and answers are summarized in Appendix 1 of the report, which is considered the most detailed evaluation of corporate governance in East Asia.

(b) ASIAN COUNTRY CORPORATE GOVERNANCE COMPLIANCE TRENDS[6]. With corporate compliance regulations and compliance laws established in each Asian country in relationship to OECD, Sarbanes-Oxley, and other international guidelines, various outside corporate institutions conducted oversight on how individual countries and companies were abiding by the rules and regulations.

For the past five years, institutions have conducted independent studies on assessing the progress of companies in meeting national and international compliance regulations.

A series of studies was conducted on selected Asian countries by the Standard & Poor's Governance Services (worldwide institution) and the Corporate Governance and Financial Reporting Centre (CGFRC) at the National University

of Singapore on corporate governance practices of country companies. Results of these findings as to compliance trends are described for the Asian countries, excluding the Philippines and Vietnam.

The Corporate Governance and Financial Reporting Centre established in January 2003 by the NUS Business School was hosted by the Department of Finance and Accounting. Its mission is to research, disseminate, and promote best practices in corporate governance and financial reporting and conduct projects in collaboration with industry and governmental organizations.

(i) Singapore. The Corporate Governance and Financial Reporting Centre (CGFRC) collaborated with Standard & Poor's (S&P's) to examine the corporate governance practices of Singaporean companies. This joint study on disclosures by STI companies regarding corporate governance practices shows that most Singapore companies have high disclosure standards.

The study involves using the corporate governance disclosure scorecard developed by S&P's to score disclosures of the corporate governance practices of the Singaporean companies. The analysis is based primarily on the disclosures made in the latest annual report.

The results of the study are published in a report entitled "Corporate Governance Disclosures in Singapore."[7] The survey looked at senior management and senior investment managers of banks, stockbroking houses, asset management companies, and insurance firms that were polled in December 2004 and January 2005.

The study assessed and focused on Singapore investor perceptions as they relate to corporate governance, for corporate governance issues are becoming key considerations for investors in deciding which Singapore companies to put their money in following recent business scandals.

The study was based on S&P's principles and practices of international corporate governance, and the companies' disclosures were taken from their annual reports, without regard for the quality and correctness of the information. The annual reports provide insight into company practices and indicate the importance of corporate governance that a company assigns itself for disclosure.

Eight key points taken from the survey of investment managers are:

1. There is an urgent need for Singapore companies to seek ways to improve accountability to stakeholders.
2. Institutional investors still put a premium on a company's financial results and strong cash reserves for their decisions, but the survey found a rising focus on companies meeting higher corporate governance standards.
3. There is an increasing emphasis on greater standards of corporate governance as well as investor communication practices in the light of recent corporate scandals.
4. Eighty-one percent of the institutional investors surveyed said good corporate governance was an incentive for investment in Singapore.

5. Corporate governance standards in the republic were higher in comparison to other Asian countries; however, as noted, "further improvement was needed."
6. A high proportion of the investors said they would like to see improvements in the enforcement of existing rules and regulations, as well as updating the current framework to reflect emerging global practices.
7. Existing government regulatory codes should have the force of law, say investment managers. With tough legislation and jail terms for wrongful disclosure common in the United States, investors say the time has come to improve Singapore's code of best practice for corporate governance.
8. When senior investment managers were asked how they view corporate governance and disclosure in investment decisions, the response was that the existing code of conduct needs to become law, and should be upgraded to better reflect global standards.

Overall the report summed up its assessment that Singapore has made significant strides in improving corporate governance, but more needs to be done.

Survey respondents rated as the most important in improving corporate governance:

1. Companies should adopt a code of conduct or ethics for all directors, officers, and employees (84 percent).
2. There should be a stricter definition of independent directors, so they are independent of management and substantial shareholders (82 percent).
3. Certain key guidelines in the current code should be made mandatory for all listed companies (83 percent).
4. Singapore government should introduce legislation to protect whistleblowers (68 percent). Survey respondents also said Singapore (Stock) Exchange (SGX) should be the regulator driving change, aided by the investment community.
5. Aside from the need for the government regulatory framework to change, corporate behavior needs to be scrutinized. There needs to be an increasing emphasis on higher standards of corporate governance as well as investor communication practices in the light of recent corporate scandals.
6. Institutional investors said their decision to invest in a company depends on the composition and quality of its board, the quality of disclosure in its financial statements, its share price, and its ability to communicate with investors.
7. The key learning point arising from this survey is the urgent need for companies to seek ways to improve accountability in terms of day-to-day management and how to better communicate this accountability to stakeholders.

(ii) Thailand. The Corporate Governance and Financial Reporting Centre (CGFRC) collaborated with Standard & Poor's to examine the corporate governance practices of Thai companies. This joint study on disclosures by Thai

SET50 Index companies regarding corporate governance practices shows there is much room for improvement.

The study involves using the corporate governance disclosure scorecard developed by Standard & Poor's to score disclosures of the corporate governance practices of the Thai companies. The analysis is based primarily on the disclosures made in the latest annual reports.

The results of the study are published in a report entitled "Corporate Governance Disclosures in Thailand: A Study of SET50 Companies." The main study findings indicate that there is need for improvement in the way companies are acting and behaving.

Findings taken from the report include eight points:

1. Corporate governance for the top Thai-listed companies remains behind international best practices, with insufficient disclosure of governance policies and too few independent directors on company boards.
2. There is considerable room for improvement if Thai companies are to meet international best practices in corporate governance.
3. While 86 percent of the companies surveyed separated the titles of board chairman and chief executive officer, few companies disclosed the relationships that directors had with the companies themselves.
4. Disclosures on the background, work history, educational qualifications, and other director positions held by board directors were absent and lacking at the majority of companies surveyed.
5. Almost half of the companies failed to disclose records of director attendance to board meetings, while 34 percent of the companies did not state whether directors were independent.
6. Use of nominees on corporate boards to represent major shareholders was a common problem affecting efforts to improve corporate governance of Asian banks.
7. Fourteen out of 50 companies also failed to disclose the number of board meetings annually, while few companies appraised the performance of their boards, and less than half of the companies maintain remuneration committees.
8. The Thai stock market SET has made steady efforts to improve corporate governance among listed companies in recent years, as listed companies are required to report their governance policies annually.

In Thailand the importance of good corporate governance is now widely recognized, with many studies demonstrating that companies with positive characteristics attract higher stock price premiums and attain better long-term performance.

(iii) Malaysia. The Corporate Governance and Financial Reporting Centre (CGFRC) collaborated with Standard & Poor's to examine the corporate

governance practices of Malaysian companies. This joint study on disclosures by Kuala Lumpur Composite Index (KLCI) companies regarding corporate governance practices shows there is much room for improvement.

The study involves using the corporate governance disclosure scorecard developed by Standard & Poor's to score disclosures of the corporate governance practices of the Malaysian companies. The analysis is based primarily on the disclosures made in the latest annual reports. The results of the study are published in a report entitled "Corporate Governance Disclosures in Malaysia," which can be downloaded at the link www.cgfrc.nus.edu.sg/publications/cg_dis_malay.htm.

"Corporate Governance Disclosures in Malaysia" noted that most companies have high boardroom independence, but there is much room for improvement in the disclosure of corporate governance practices. The study noted that in market capitalization terms Malaysia showed considerable variation in its disclosure practices. To quote from the report:

"Judging from scores, there seems to be much room for Malaysian companies to improve disclosures of their corporate governance practices," the report authors noted in issued statement. Only three companies disclosed that they evaluated the individual performance of board members, but they gave no details on the criteria used to assess a board member's performance.

All 100 companies on the KLCI were ranked by their market capitalization and the top 50 companies from this list were chosen, because international investors are likely to have strong interest in them by virtue that they are part of the index. These companies are expected to practice relatively higher standards of corporate governance compared with other listed Malaysian companies and can be role models of corporate governance for the others.

The majority of Malaysia's top 50 largest companies failed to make the grade in corporate governance disclosures. Most of the companies' audit, remuneration, and nomination committees were still far from independent, while there was a lack of transparency in how board members were chosen.

Of the 50 companies, there was a large difference between the top five companies relative to the other KLCI companies in that the top five had better disclosures of their overall corporate governance practices. There was little variation in scores among these five companies but significant differences between them and the other 45. The top five companies had better disclosures on their nomination and remuneration committees, scheduled more committee and board meetings, and organized formalized training for new directors.

Findings were that most Malaysian companies have high boardroom independence, but there is much room for improvement in disclosure of corporate governance practices, Standard & Poor's said. "Judging from scores, there seems to be much room for Malaysian companies to improve disclosures of their corporate governance practices," as noted in the report.

The co-director of CGFRC said one of the areas in which Malaysian companies could improve was the independence of the directors of the board and the board committees to have a better corporate governance practices. "We found that this is the other key area [in which] Malaysian companies were found lacking in the corporate governance practices."

The top five Malaysian companies have better disclosure than the rest of surveyed companies. However, they were found lacking in several respects:

- The number of independent directors was seldom a majority, and none had more than two-thirds who were independent.
- Only one had an audit committee comprised entirely of independent directors. Also, just one had a wholly independent remuneration committee, and none of the five had a nominating committee whose members were all independent.
- Independent access to management was lacking. Only two provided the directors and the board with independent access to management and disclosed this in the annual report.
- Evaluation of board members was lacking. Only three disclosed that they evaluate the individual performance of directors. None provided details in the annual report on the criteria used to assess directors' performance.
- Only two out of the five disclosed the types of material transactions that the board must approve.
- None of the top five companies recorded 100 percent attendance at their board of directors meetings.
- Only three of the top five companies disclosed that they evaluate the individual performance of board members. Furthermore, none of them provided details in the annual report on the criteria used for assessing board member performance.

(c) COUNTRY CORPORATE GOVERNANCE COMPLIANCE TRENDS—PHILIPPINES AND VIETNAM. This section describes compliance trends of the Philippines and Vietnam outside of the studies and reports conducted by Standard & Poor's Governance Services (worldwide institution) and the Corporate Governance and Financial Reporting Centre (CGFRC) at the National University of Singapore.

(i) Philippines. The largest accounting firm in the Philippines, SGV, noted that the regulatory framework advocating the principles of good governance among corporations is definitely a step in the right direction. It sets the tone and the overall macro-level infrastructure that tells investors and stakeholders that the country is serious in setting the groundwork for a desirable investment destination.

For at the micro or firm level, real corporate governance goes beyond compliance with regulatory requirements. It is about companies' corporate directors,

senior management, and employees working together to be true to the spirit and not just the letter of the code.

(ii) Vietnam. The Vietnam situation regarding corporate governance is not covered by ACGA or the Singapore Financial Reporting Center. A recent survey of 85 large enterprises in Vietnam indicated that corporate governance is a relatively new concept in the country. In response to a study conducted by World Bank affiliates, 23 percent of the respondents said they had a "certain understanding" of corporate governance, although most company directors admitted it was yet to be adopted in Vietnam.

The Vietnam Chamber of Commerce and Industry noted that a wide range of ownership structures existed in Vietnam, each of them governed by a different set of laws. Regulations on corporate governance also differed for different kinds of businesses, with many of them even contradicting each other, making corporate governance a difficult task, the chamber said.

Chairman Ha Noi Milk of the Joint Stock Company said that since the heads of most private companies did not possess corporate management knowledge or skills, they did not realize that good corporate governance would enable their enterprises to develop and attract investment.

Nguyen Dinh Cung, of the Central Economics Management Institute, said that standardized corporate management rules were yet to make an appearance at state-owned enterprises. Consequently, managers' obligations were unclear, making them less accountable for their companies' efficiency.

"One of the most important regulations relating to corporate governance is for companies to publish business information and periodically audit financial accounts," Cung said, but unfortunately most Vietnamese enterprises fail to do so.

Nguyen Son, deputy head of the State Securities Commission's Market Development Board, spelled out two reasons for Vietnamese companies lacking corporate governance:

1. The economy still contained nonmarket elements, with the government continuing to be a benefactor of many enterprises in terms of providing capital, raw materials, and pricing.
2. A level playing field was lacking for the corporate sector; the legal environment was not truly level for state-run and nonstate enterprises, and rules governing disclosure of information and auditing were not equitable between listed and unlisted companies.

Finally, these two factors meant there was no incentive for companies to adopt corporate governance, and managers and government agencies had little understanding of the importance and benefits of corporate governance.

The basic tenet was that the government should pass laws forcing companies to adopt standard corporate management rules, particularly with regard to disclosing information and audit.

Ha Noi Milk of the Joint Stock Company said good corporate governance was very important to Vietnamese enterprises of all kinds. Company managers learned of advanced corporate governance models to improve both awareness and capability in the field.

The recommendation was that Vietnamese companies should be allowed to hire corporate governance specialists as advisers and participate in enterprise support programs organized by nongovernmental organizations.

(d) CORPORATE GOVERNANCE IN ASIA 2005. A detailed report on corporate governance was produced in collaboration with the Asian Corporate Governance Association (ACGA), an independent nonprofit organization working on behalf of all investors to improve corporate governance practices in Asia.

CLSA Asia-Pacific Markets (an investment firm; www.clsa.com) conducted the study where the ACGA endorsed the methodology and contributed to the country analysis and did not participate in the assessments of companies, for which CLSA retains the responsibility.

The survey was conducted on corporate governance issues and progress in ten Asia markets except-Japan, which was covered by CLSA.

The report has details of the survey, and in this section findings from the report are described.

(i) Malaysia—Work in Progress. Following accelerated rate of reforms in 2001–2003, the Malaysian corporate governance environment over recent years has not seen much major change and remains a work in progress. There were no major issues confronted in the country. Generally, we note positive momentum on the corporate governance reform front and firm political will to increase corporate transparency. Enforcement remains a major corporate governance issue, as has been the case for some time. More could always be done on this front, but this is a subjective element.

(ii) Philippines—Chugging Along. The Philippines has taken measures to improve corporate governance with the implementation of the Securities Regulation Code (SRC) in 2000 and the Code of Corporate Governance (CCG) in 2002.

The central bank, by using its regulatory powers, has mandated corporate governance briefings for banks covering the anti-money laundering act (AMLA). Additional legislation to prevent corporate fraud and abuse, in the form of the Corporate Reform Act, is still finding its way through Congress. In practice, a lot needs to be done to instill the right culture and commitment to corporate governance. Specifically, laws and policy framework look good on paper but there is more to be desired in terms of implementation and enforcement of these laws.

(iii) Singapore—Emerging from Mishaps. During 2005, Singapore had more than its fair share of corporate governance problems. This raised investor concern; however, the country retains its position in CLSA's annual corporate governance

survey, although the gap has narrowed significantly based on the more stringent country questionnaire adopted this year.

In Singapore's favor are greater independence for the board of directors and widespread awareness of corporate governance at local firms. Regulators are tightening rules, but perhaps more can be done and corporate governance for Singapore companies has improved.

(iv) Thailand—Enforcement Issues. The Thai market in 2005 had its share of corporate governance scandals. The country score for corporate governance in Thailand declined based on a series of scandals. Thailand continues to score weakly in enforcement and corporate governance culture. No survey sections have seen any real improvement from the preceding year. The score for accounting standards has fallen significantly, although this is largely due to more stringent criteria.[8]

The Asian Roundtable on Corporate Governance was held to obtain contributions of numerous organizations and individuals such as the World Bank Group, the Asian Development Bank, Asian institutions, national securities commissions, the private sector, and all other representatives in the region.

The paper noted that good corporate governance is widely recognized as essential for establishing an attractive investment climate describe by competitive companies and efficient financial markets. Good corporate governance is also critical to economies with extensive family-business ownership because of its role in facilitating management succession and promoting entrepreneurship.

The roundtables employed the OECD Principles of Corporate Governance as a framework for developing a regional White Paper or comparative paper on corporate governance. A quick-reference table on the corporate governance framework in Asia can be found in the aforementioned White Paper. The White Paper's priorities for reform reflect the discussions and recommendations of those meetings, which took place from 1999 to 2003.

These priorities are highlighted here, and details can be obtained from the report.

Priority 1: Public- and private-sector institutions should continue to raise awareness among companies, directors, shareholders, and other interested parties of the value of good corporate governance.

Priority 2: All jurisdictions should strive for effective implementation and enforcement of corporate governance laws and regulations.

Priority 3: Asian Roundtable countries should work toward full convergence with international standards and practices for accounting, audit and nonfinancial disclosure. Where, for the time being, full convergence is not possible, divergences from international standards and practices (and the reasons for these divergences) should be disclosed by standards setters; company financial statements should repeat or reference these disclosures where relevant to specific items.

Priority 4: Boards of directors must improve their participation in strategic planning, monitoring of internal control systems, and independent review of transactions involving managers, controlling shareholders, and other insiders.

Priority 5: The legal and regulatory framework should ensure that noncontrolling shareholders are protected from exploitation by insiders and controlling shareholders.

Priority 6: Governments should intensify their efforts to improve regulation and corporate governance in Asian banks.

(e) LESSONS LEARNED—COMPLIANCE TRENDS IN TECHNOLOGY IT GOVERNANCE. In 2003, PricewaterhouseCoopers (PWC) was commissioned by the Information Technology Governance Institute (ITGI) to conduct the first global research into awareness, perceptions, and applications of IT governance and IT governance frameworks. This was followed in 2005 by the ITGI conducting the second global survey on IT governance, and the report highlights the most significant findings.

It is critically important to the Asian countries to ensure that IT governance is complied with based on its governance program.

The purpose of the research was to contact corporate members to determine their sense of priority and actions already taken relative to IT governance and their need for tools and services to help assure effective IT governance. Briefly, the project findings were:

- Information technology is more critical to business than ever.
- General managers feel more positive toward IT than IT managers do.
- Significant differences among industry sectors exist.
- IT security is *not* the most important IT-related problem.
- Awareness of CobiT compliance has increased.
- Sarbanes-Oxley has not created the anticipated effect.
- IT governance (and CobiT) is not as easily implemented as originally estimated.

48.3 CORPORATE GOVERNANCE PERFORMANCE AND COMPLIANCE IN ASIA[9]

The lack of effective corporate governance is widely viewed as one of the structural weaknesses that were responsible for the outbreak of the 1997 Asian financial crisis. In companies controlled by family owners, these owners could pursue their private interests relatively easily and often at the expense of minority shareholders and firms' profits.

Since the crisis there has been high priority to putting sound regulatory frameworks in place. However, there are critics who believe the reform measures, based largely on the Anglo-American model, to be cosmetic because of the concentrated ownership structure and the embedded Asian institutional and sociocultural norms in local economies.

One thesis approached in the report was there was little evidence provided about the beneficial effect of good corporate governance on firms' values and performance in these economies. In Asian culture, stakeholders other than shareholders, especially employees and creditor banks, can also play a useful role in corporate governance.

The authors addressed these questions by conducting a firm-level questionnaire survey in four countries particularly hard hit by the Asian crisis: Indonesia, the Republic of Korea, Malaysia, and Thailand.

Trends are difficult to identify, but there has been some oversight of corporate governance in Asia conducted at the Asian Development Bank Institute (ADBI). Corporate governance is one of the key research areas of ADBI from 1997 resulting from the Asian financial crisis, which was to a large extent attributable to poor corporate governance.

Although not including other countries, the report provides for a good understanding of actual corporate practices rather than of rules and regulations that may not be followed in practice.

The survey covers two areas not specifically focused on in previous reports with two main elements: (1) shareholders' rights and information disclosure and (2) the effectiveness of boards of directors.

Corporate secretaries responded to the first questionnaire, and for the second element, corporate secretaries responded in relation to factual information and executive directors and independent directors were asked to provide opinions.

The survey had three broad objectives:

1. Investigating corporate governance practices at the firm level in comparison with the relevant regulatory framework for deeper understanding of corporate governance
2. Evaluating the relationship between corporate governance practices and firm performance
3. Assessing the potential roles of stakeholders other than shareholders in corporate governance

The major findings of the study were:

- The gap between the regulatory framework and formal corporate governance practices is probably not particularly large, but a substantial gap does exist between the regulatory framework and practices in substance or spirit.
- Larger gaps and variations are apparent in areas where regulations or guidelines are less demanding or enforcement is difficult, such as requirements pertaining to the provision of information to and support for directors and the functions and activities of the board or of board committees.
- Clearly, corporate governance matters. In evaluating the quality of firms' corporate governance, the market seems to differentiate largely on the basis

of substance, discount for the observed quality of corporate governance for firms run by controlling families, and take into account good corporate governance in countries where the legal and judicial systems for investor protection are weak.

- For firms surveyed, corporate governance scores are strongly associated with firm performance as measured by Tobin's Q (measured as the ratio of market value to book value of a firm).
- Scores for shareholders' rights alone do not show any significant association with firm performance, whereas scores for board effectiveness and overall scores (average scores for shareholders' rights and board effectiveness) turn out to be significant.
- The evidence also supports the view that corporate governance matters more in countries where the legal and judicial systems for protecting investors are weak.
- In all four countries, boards seem to be somewhat inactive in selecting, monitoring, and replacing CEOs and reviewing the remuneration of key executives and directors.

The study's conclusions were:

- Diffused ownership is relatively rare in all the countries under study except for Malaysia. Professional managers in CEO positions are found in less than 60 percent of the Malaysian firms and in only 40 to 50 percent of the respondent firms in three other countries. Major corporate governance concern in listed firms is needed to prevent controlling owners from expropriating minority shareholders.
- Surveyed firms are doing relatively well in recognizing the rights of shareholders. This may be due to the fairly elaborate laws and regulations on shareholders' rights and the operation of shareholders' meetings. Nevertheless, there is substantial room for improvement.
- Shareholders are inadequately protected with rights to priority capital subscription and the approval of major related-party transactions, as well as dissenters' rights. Voting by mail is largely unavailable, and minority shareholders seem to take little part in the process of selecting board members.
- Sample firms perform relatively poorly in relation to information disclosure and transparency, particularly for matters potentially involving self-dealing or other conflicts of interest. In Indonesia and Thailand, web sites are not yet fully utilized as a way to disclose information in a timely manner and enhance transparency.
- Thai boards of directors seem to be too large with too few independent directors, while Indonesian boards are probably too small. The positions of CEO and board chairperson are separated in more than 80 percent of the Malaysian and Thai firms because of the two-tier board system. This results from the fact that directors are effectively selected by the CEO or

controlling owner, while cultural factors such as personal relationships or behavioral norms play a relatively small role.

- Functions of boards and board committees in the countries are generally weak, even though corporate directors tend to agree that their boards are a forum for serious discussion of significant corporate matters. In all four countries, boards seem to be somewhat inactive in selecting, monitoring, and replacing CEOs and reviewing the remuneration of key executives and directors.
- Corporate governance matters more in countries where the legal and judicial systems for protecting investors are weak. The market valuation of companies is also associated with employee participatory practices, including shop-floor activities and participation in financial matters.
- Among the various components of corporate governance practices, what appear to be the most significant are support for and evaluation of outside directors. This is the area where the sample firms generally score most poorly.
- The results indicate that how adequately independent directors are supported and evaluated for their best contribution to the company is more important than the superficial board structure, such as the share of independent directors. This finding is consistent with the respondents' view that the highest priority for having more effective boards is the timely provision of relevant information to directors.
- Overall, the survey results indicate that a big gap between the regulatory framework and actual corporate governance practices probably does not exist in form, but that a substantial gap exists in substance or spirit.
- Understandably, larger gaps and variations exist in areas where regulations and guidelines are less demanding or enforcement is difficult, such as supporting and evaluating outside directors and the specific functions of the board or of board committees.
- There is clear evidence that corporate governance matters in the valuation of firms and that the market seems to be smart in evaluating the quality of firms' corporate governance, in that it tends to differentiate among firms more on the basis of substance than of form.
- The findings indicate that the Anglo-American corporate governance framework does work. Even though firms in the countries under review may not embrace the model wholeheartedly, the market obviously discriminates among firms according to the model's standards, suggesting that firms will move toward meeting more of these standards.
- A stakeholder model appears to be less promising in firms that are substantially foreign owned or have already embraced the Anglo-American model with higher corporate governance scores. For firms controlled by a single family, the potential corporate governance role of employees tends to be better recognized, while that of banks is not very welcome.

- Many of the institutions now being built, with relevant legal, accounting, and audit systems, are likely to form the basic infrastructure for any workable models, and existing cultural norms and corporate cultures might be more favorable for a stakeholder model.
- Policy implication of the survey results is that the ongoing corporate governance reform efforts should be continued to encourage firms to pay more attention to substance than to form.
- To enhance the board's effectiveness, the provision of adequate support for outside directors is the most important factor, as well as the promotion of a boardroom culture that encourages constructive criticism and alternative views.
- As indicated by the respondents, priorities should be given to making internal corporate governance mechanisms work better and enhancing the standards for information disclosure, accounting, and auditing.

48.4 LESSONS LEARNED—BEST PRACTICES

Studies conducted on corporate governance identified key factors that serve as lessons learned and best practices to be considered as guidance for governments and at corporate settings.

(a) LESSONS LEARNED. The lesson findings resulted from the APEC study include:

- Ranking on rules and regulations and ranking of investor evaluation on the quality of corporate governance practices are not significantly correlated. The result implies that there are significant differences between what the rules and regulations intend and how corporate governance is actually practiced by corporations in each economy.
- Corporate governance rules and regulations are not enforced in some economies as they are supposed to be.
- Economies that practice poor corporate governance have introduced new rules and regulations to improve corporate governance. Results *should not* be interpreted as causality between corporate governance rules and regulations and corporate governance practices.
- East Asian economies have made a significant effort to improve their corporate governance practices. A regulatory structure for corporate governance is reasonably constructed.

(b) BEST PRACTICES FOR THE FUTURE. Studies conducted on corporate governance identified four key factors that serve as best practices to be considered as guidance for governments, and at corporate settings.[10]

1. National government economies should concentrate their efforts on implementation and enforcement of rules and regulations; from now on they really intend to improve their corporate governance practices.

2. National government economies rank first and second respectively in the evaluation of rules and regulations, but they are ranked lower in the investor survey.
3. National government economies made significant efforts in introducing rules and regulations so as improve corporate governance, but they should also make additional efforts to implement and enforce these rules and regulations.
4. Next phase should be implementation and enforcement of the new rules and regulations. Investor relations are another important area that could help change investors' perceptions.

(c) PROTECTING INVESTORS—LESSONS LEARNED[11]. The World Bank's "Doing Business" database provides objective measures of business regulations and their enforcement. The database indicators are comparable across 155 national economies, indicating that regulatory costs of business can be used to analyze specific regulations that enhance or constrain investment, productivity, and growth.

"Doing Business" measures the strength of minority shareholder protections against directors' misuse of corporate assets for personal gain. The indicators distinguish three dimensions of investor protection: The data come from a survey of corporate lawyers and are based on company laws, codes of civil procedure, and securities regulations

Exhibit 48.1 shows the main indicators of robust internal controls. They include:

- Transparency of transactions (extent of disclosure index)
- Liability for self-dealing (extent of director liability index)
- Shareholders' ability to sue officers and directors for misconduct (ease of shareholder suit index)
- Strength of investor protection index (the average of the three indexes)

(d) LESSONS LEARNED/BEST PRACTICES. One of the latest reports on the assessment of corporate governance in Asia was presented in 2005 by the Asian Corporate

Region or Economy	Disclosure Index	Director Liability Index	Shareholder Suits Index	Investor Protection Index
East Asia & Pacific	5.6	4.2	6.2	5.3
South Asia	4.1	4.6	6.4	5.0
Malaysia	10	9	7	8.7
Philippines	1	2	7	3.3
Singapore	10	9	9	9.3
Thailand	10	2	6	6.0
Vietnam	4	1	2	2.3

EXHIBIT 48.1 GOVERNANCE INDICATORS: MAJOR S. E. ASIAN ECONOMIES

Governance Association (ACGA).[12] Here are four findings focused by the director of the ACGA.

1. Asian country scores (2005) trended downwards, but not due to a decline in objective corporate governance standards or less effort on the part of regulators.
2. Weaknesses in the detail of laws and regulations have become more apparent.
3. A gap exists between national accounting policies and practices.
4. Corporate governance best practices are not gaining traction among listed companies.

These findings indicate the status of key issues that represent Asian corporate governance:

Rules and Regulations: Issues

- Quarterly reporting: mandatory, but not always sufficient
- Audit committees: mandatory, but not always implemented
- Audit committees: questions as to whether they are functioning independently and effectively
- Securities laws not deterring insider trading and market manipulation
- Preemption rights of investors not firmly protected

Enforcement: Issues

- Perception in many markets that regulators do not treat companies equally
- Limited disclosure by regulators of their enforcement track records (although some countries are impressive)
- Limited regulatory track record against insider trading
- Limited voting by institutional investors (although on the rise)

Political and Regulatory Environment: Issues

- Are securities regulators sufficiently autonomous from government?
- Lingering questions over regulatory structure, especially with regard to stock exchanges
- Unavailability of laws and regulations in English in some markets
- Ineffective access to courts—high costs, limited legal remedies

Corporate Governance Culture: Issues

- Does the average listed company believe corporate governance is of value? ("No" or "marginally" in most markets)
- Are large-cap companies following the spirit of corporate governance rules? (50–50)
- How many companies have truly independent chairmen? (Very few)

- Is disclosure of internal controls by listed companies sufficient? ("No" or "marginally")

Areas of Strength: Rules

- Considerable improvement in financial reporting standards in most markets
- Rules on disclosure of material transactions and substantial ownership generally good
- Voting by poll moving onto the agenda, if not yet a rule in most markets; Voluntary voting by poll in some markets (notably Hong Kong)
- Legislative improvements planned in some countries (e.g., China is planning to amend its Company Law)

Areas of Strength: Enforcement

- Recognition that regulators are investing more effort in enforcement; increase in investigations, prosecutions, settlements
- Increased supervision of intermediaries (e.g., brokers, advisers) and initial public offerings (IPOs) (e.g., quality of prospectus disclosure)
- Anecdotally, some increase in institutional investor voting (although no statistics available)

Areas of Strength: Political/Regulatory

- Stock exchanges have become extremely useful sources of information on listed companies. Most now provide extensive online databases of issuer reports, announcements, and notices—although not necessarily in English!
- The degree of media freedom to report on corporate governance issues does appear to be on the rise.

Areas of Strength: Corporate Governance Culture

- In addition to the large-cap companies, a small group of mid-caps is gaining a reputation for good governance.
- Remuneration of independent directors is on the rise.
- Improvement in internal controls and the practice of risk management.
- Some Asian companies are starting to appoint independent board chairs.

Recommendations

- Review problematic rules and procedures with market participants (e.g., preemption rights, voting systems, shareholder meetings). Ask the market what it thinks is important. It is hard for market discipline to function on an unlevel playing field.
- If mandatory rules are sound (e.g., audits), ensure they are: (1) implemented, and then (2) properly implemented!

Country[1]	2000	2001	2002	2003[2]	2004[3]
Singapore	7.5	7.4	7.4	7.7	7.5
Hong Kong	7.1	6.8	7.2	7.3	6.7
India	5.6	5.4	5.9	6.6	6.2
Malaysia	3.2	3.7	4.7	5.5	6.0
Korea	5.2	3.8	4.7	5.5	5.8
Taiwan	5.7	5.3	5.8	5.8	5.5
Thailand	2.8	3.7	3.8	4.6	5.3
Philippines	2.9	3.3	3.6	3.7	5.0
China	3.6	3.4	3.9	4.3	4.8
Indonesia	2.9	3.2	2.9	3.2	4.0

1. Ranked in descending order according to 2004 score. Scores out of 10.
2. First year in which ACGA collaborated with CLSA.
3. Introduced more rigorous scoring methodology in 2004.

ACGA

Source: ''CG Watch,'' a joint report by CLSA Asia-Pacific Markets and ACGA.

EXHIBIT 48.2 S.E. ASIA GOVERNANCE INDICATORS: 2000–2004

- Improve disclosure of enforcement track record. Better enforcement leads to higher trust in the stock market.
- Ensure all major laws and regulations are translated and easily accessible.
- Ask companies and investors to rate the value of different best practices/corporate governance rules. What works? What doesn't?

In Exhibit 48.2, ranking by country is in descending order according to 2004 score (out of a score of 10). This was the first year in which the Asian Corporate Governance Association (ACGA) collaborated with CLSA Asia-Pacific Markets. The study had more rigorous scoring methodology the next year.

(e) IT MANAGEMENT ASPECTS OF LESSONS LEARNED. Management of corporate governance is an important factor in meeting government regulations and laws guiding corporations.

Lessons learned from studies conducted on the impact of national corporate governance programs are identified:

- Management should align business and IT strategy and goals down into the enterprise and translate them into action for employees at each level.

- After aligning business and IT strategy, management should align IT and the business organization, promoting coresponsibility for the success of IT projects and the return of business value.
- Management should ensure that risk analysis is an integral part of all planning processes, focusing on the vulnerabilities of the IT infrastructure, the exposure of intangible assets to security and operational risks, and the risk of IT project failures.
- Management should implement performance measurement based on the aligned strategy and goals.

The CIO should have influence to make these steps happen; the CIO has the position of authority in the organization and holds the power to say yes or no.

48.5 CONCLUSION

The Southeast Asian countries identified in this report represent many issues that are paramount in countries and the private sector that need immediate attention.

Present information and reports are diverse and cover specific areas as designated in the individual study focus. Therefore, to line up the same study covering all countries at the same time is difficult, if not impossible.

Overall national governments need to assess the present corporate governance policies and consider new and updated laws and regulations.

Government regulatory institutions need to look at how the present laws and regulations are working and propose changes as appropriate through the regulatory process.

Private sector corporations need to implement the law and regulations guiding corporate governance, as well as adhere to the present guidelines of corporate governance guiding their industry.

Public and private sector education and training are needed to raise the level of knowledge and competence of all parties concerned.

The reader should consider the results of each study and area covered for further work.

Notes

1. "The Economic Crisis in East Asia: Causes, Effects, Lessons," by Martin Khor, director, Third World Network (1998). www.ifg.org/khor.html.
2. "White Paper on Corporate Governance in Asia." www.oecd.org/dataoecd/4/12/2956774.pdf.
3. "Evaluation of Corporate Governance in East Asian Economies," submitted by PECC, 12th APEC Finance Ministers' Meeting, Jeju, Korea, September 2005; "Evaluation of Corporate Governance in East Asian Economies: Report of a PECC Finance Forum Task Force on Macroeconomic Corporate Governance Scorecard," by Stephen YL Cheung, professor of finance, City University of Hong Kong (e-mail: EFSTEVEN@cityu.edu.hk), and Hasung Jang, dean, Korea University Business School (e-mail: jangya@chol.com).

4. "Evaluation of Corporate Governance in East Asian Economies," submitted by PECC, 12th APEC Finance Ministers' Meeting, Jeju, Korea, September 2005.
5. Questionnaire was based on White Paper on Corporate Governance in Asia published by the OECD in 2003. Authors selected questions that were relevant to Asian economies but added number of questions that are not included in the White Paper. Survey period conducted during the period from May 2005 to August 2005.
6. "Evaluation of Corporate Governance in East Asian Economies," submitted by PECC, 12th APEC Finance Ministers' Meeting, Jeju, Korea, September 2005; "Evaluation of Corporate Governance in East Asian Economies: Report of a PECC Finance Forum Task Force on Macroeconomic Corporate Governance Scorecard Preliminary Report," revised September 2, 2005, by Stephen YL Cheung, professor of finance, City University of Hong Kong (e-mail: EFSTEVEN@cityu.edu.hk) and Hasung Jang, dean, Korea University Business School (e-mail: jangya@chol.com).
7. www.cgfrc.nus.edu.sg/publications/cg_dis_sg.htm.
8. "The Asian Roundtable on Corporate Governance: A White Paper on Review of Regional Aspects of CG." www.oecd.org/dataoecd/48/55/25778905.pdf.
9. Sang-Woo Nam and Il Chong Nam, "Corporate Governance in Asia: Recent Evidence from Indonesia, Republic of Korea, Malaysia, and Thailand," Asian Development Bank Institute, October 2004.
10. 12th APEC Finance Ministers' Meeting (Korea, September 2005), report was submitted on Evaluation of Corporate Governance in East Asian Economies as part of PECC Finance Forum Task Force on Macroeconomic Corporate Governance Scorecard.
11. www.doingbusiness.org/ExploreTopics/ProtectingInvestors/.
12. Asian Corporate Governance Association (ACGA), "A Preview of CG Watch 2005," presentation by Jamie Allen, Secretary General, at the OECD 2005 Asian Corporate Governance Roundtable, September 8, 2005, Bali.

CHAPTER 49

AUSTRALIAN CORPORATE GOVERNANCE: THE ASX PRINCIPLES

Anthony Tarantino, PhD

49.1 AUSTRALIAN MODEL OF CORPORATE GOVERNANCE

Australia has taken an approach to corporate governance and improved internal controls that should be considered a role model. In our World Bank ratings of six elements of corporate governance, Australia scores very highly against the top gross domestic product (GDP) nations and against its neighbors in East Asia and Southeast Asia.

Australia has created corporate guidance based on best practices for ten key process areas. Companies may chose to not follow the recommended best practices, but must explain why. Formed in August 2002, the Australian Stock Exchange (ASX) Corporate Governance Council brought together 21 professional and business groups with the mission "to develop and deliver an industry-wide, supportable, and supported framework for corporate governance which could provide a practical guide for listed companies, their investors, the wider market and the Australian community.... The size, complexity, and operations of

companies differ, and so flexibility must be allowed in the structures adopted to optimize individual performance. That flexibility must, however, be tempered by accountability—the obligation to explain to investors why an alternative approach is adopted—the 'if not, why not?' obligation. The enhancement of corporate accountability and the adoption of this framework for reporting is a major evolution in corporate governance practice in Australia. The impact on Australian companies must not be underestimated."[1]

The guideline approach takes into consideration that a checklist and one-size-fits-all approach is unrealistic, something that the Securities and Exchange Commission (SEC) and Public Company Accounting Oversight Board (PCAOB) only acknowledged in the spring of 2005. According to the ASX March 2003 introduction, "it states aspirations of best practice for optimizing corporate performance and accountability in the interests of shareholders and the broader economy. If a company considers that a recommendation is inappropriate to its particular circumstances, it has the flexibility not to adopt it, a flexibility tempered by the requirement to explain why. Companies are encouraged to use the guidance provided by this document as a focus for reexamining their corporate governance practices and to determine whether and to what extent the company may benefit from a change in approach, having regard to the company's particular circumstances.

"There is little value in a checklist approach to corporate governance that does not focus on the particular needs, strengths, and weaknesses of the company. The Council recognizes that the range in size and diversity of companies is significant and that smaller companies may face particular issues in attaining all recommendations from the outset. Performance and effectiveness can be compromised by material change that is not managed sensibly. Where a company is considering widespread structural changes in order to meet best practice, the company is encouraged to prioritize its needs and to set and disclose best practice goals against an indicative time frame for meeting them."

Disclosure requirements. "Companies are required to provide a statement in their annual report disclosing the extent to which they have followed these best practice recommendations in the reporting period.[2] Where companies have not followed all the recommendations, they must identify the recommendations that have not been followed and give reasons for not following them. Annual reporting does not diminish the company's obligation to provide disclosure."[3]

What disclosures are necessary? "It is only where a recommendation is not met or where a disclosure requirement is specifically identified that a disclosure obligation is triggered. Each recommendation is clearly identified as such. The commentary and guidance that follows each recommendation does not form part of the recommendation. It is provided to assist companies to understand the reasoning for the recommendation, highlight factors which may be relevant for consideration, and make suggestions as to how implementation might be achieved."

Where should disclosure be made? "Specific guidance is given at the end of each principle as to what disclosure the company is required or encouraged to make and where. In some cases, the company is required to set out the relevant disclosure in a separate corporate governance section of the annual report. Where the Corporations Act requires particular information to be included in the directors' report, the company has the discretion to include a cross-reference to the relevant information in the corporate governance section of the annual report rather than replicating that information." According to Australia's Treasury Department "it is the responsibility of company boards of directors to certify that a company's financial statements comply with accounting standards, and provide an accurate view of its financial condition. The Corporations Act provides for a broad fiduciary responsibility of directors. The Act also requires auditors to form an opinion as to whether a company's financial statements comply with accounting standards and provide a view of its financial condition."[4]

What is the disclosure period? "The change in reporting requirement applies to the company's first financial year commencing after 1 January 2003. Accordingly, where a company's financial year begins on 1 July, disclosure will be required in relation to the financial year 1 July 2003–30 June 2004 and will be made in the annual report published in 2004. Companies are encouraged to make an early transition to the best practice recommendations and are requested to consider reporting by reference to the recommendations in their corporate reporting this year."

What disclosures are necessary? "It is only where a recommendation is not met or where a disclosure requirement is specifically identified that a disclosure obligation is triggered. Each recommendation is clearly identified as such. The commentary and guidance that follows each recommendation does not form part of the recommendation. It is provided to assist companies to understand the reasoning for the recommendation, highlight factors which may be relevant for consideration, and make suggestions as to how implementation might be achieved."

Where should disclosure be made? "Specific guidance is given at the end of each principle as to what disclosure the company is required or encouraged to make and where. In some cases, the company is required to set out the relevant disclosure in a separate corporate governance section of the annual report. Where the Corporations Act requires particular information to be included in the directors' report, the company has the discretion to include a cross-reference to the relevant information in the corporate governance section of the annual report rather than replicating that information."

49.2 WORLD BANK CORPORATE GOVERNANCE RATINGS

The World Bank publishes governance ratings for over 200 nations. The evaluation is based on six elements of compliance. (See Exhibit 49.1.) The latest ratings are for 2005 and represent one of the most viable means of comparing

2005 World Bank—Six Elements of Governance								
Nation	Average	Top GDP 2005 Rank	Voice & Accountability	Political Stability	Gov't Effectiveness	Regulatory Quality	Rule of Law	Control of Corruption
Australia	**91.67%**	**2**	90%	82%	92%	94%	96%	96%
Brazil	**49.82%**	**11**	57%	41%	55%	55%	43%	48%
Canada	**92.33%**	**1**	95%	79%	96%	95%	95%	94%
China	**35.57%**	**14**	6%	39%	52%	45%	41%	31%
France	**83.58%**	**6**	92%	59%	90%	80%	90%	91%
Germany	**88.08%**	**3**	94%	67%	90%	90%	94%	94%
India	**45.57%**	**13**	56%	22%	52%	41%	56%	47%
Indonesia	**27.50%**	**16**	41%	9%	37%	37%	20%	21%
Italy	**68.32%**	**10**	77%	53%	72%	76%	64%	68%
Japan	**83.33%**	**7**	75%	80%	85%	86%	89%	85%
Mexico	**48.93%**	**12**	54%	36%	57%	62%	40%	44%
Russia	**29.45%**	**15**	26%	19%	39%	44%	22%	28%
S. Korea	**70.18%**	**9**	68%	61%	79%	72%	73%	69%
Spain	**83.27%**	**8**	87%	60%	90%	88%	85%	90%
UK	**88.07%**	**4**	93%	59%	94%	94%	93%	95%
US	**84.48%**	**5**	90%	49%	92%	93%	92%	92%

Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2005'' (September 2006).

EXHIBIT 49.1(a) WORLD BANK 2005: SIX ELEMENTS OF GOVERNANCE

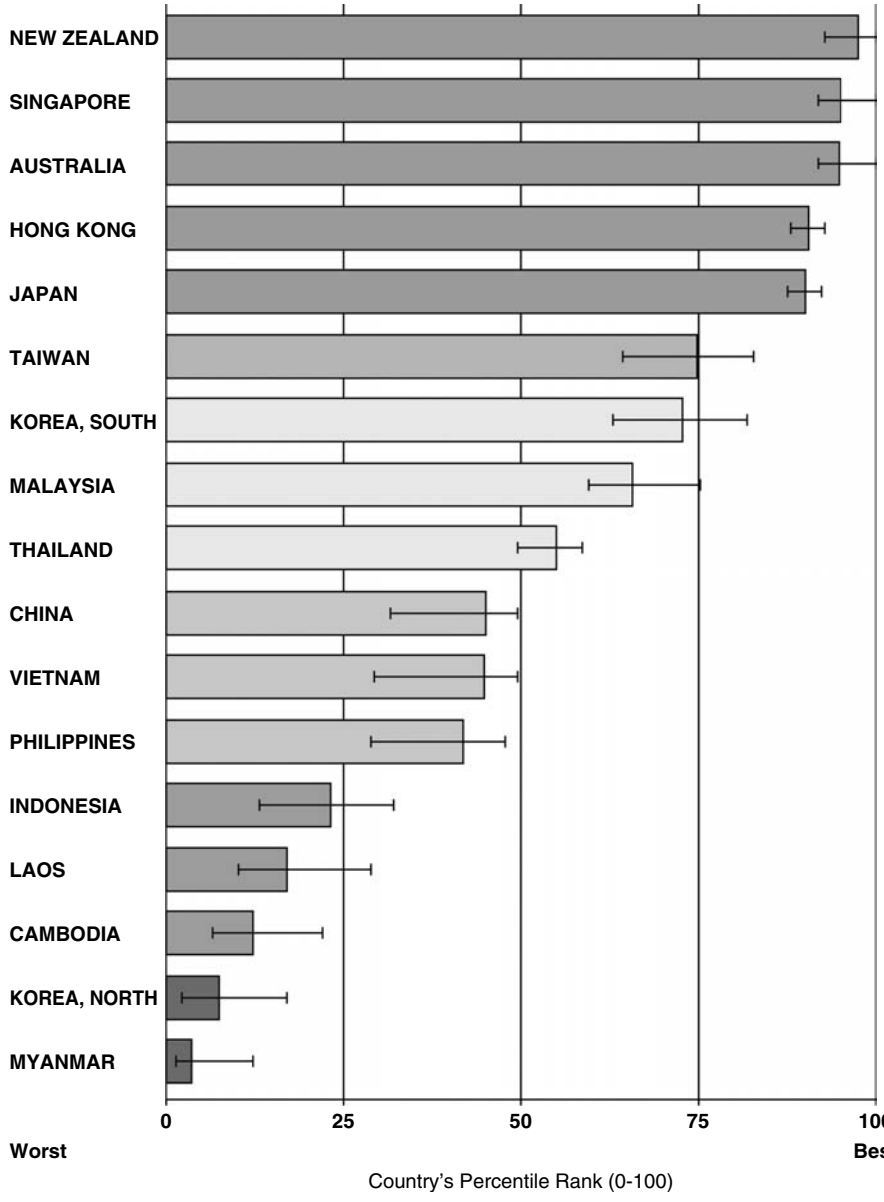
nations. The World Bank correctly assumes that corporate governance does not exist in a vacuum and can prosper only with factors that exist outside of corporations: political stability/lack of violence, government effectiveness, rule of law, corruption control, voice and accountability, along with regulatory quality. By these criteria, Australia enjoys very high levels of corporate governance and scores well in all six categories against the top 16 GDP nations as measured by purchasing power parity (PPP).

The World Bank percentile rank changes from 2005, 2004, 2003, 2000, 1998, to 1996 (top to bottom order) for the six elements of governance are shown in Exhibit 49.2 and show only the area of political stability/no violence losing ground in the past ten years.[5]

The World Bank percentile rank compares Australia's regulatory quality to with its neighbors in Southeast and East Asia, as shown in Exhibit 49.3.[6]

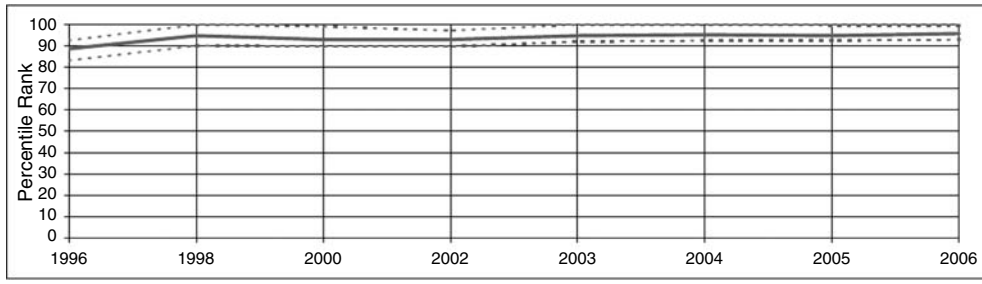
49.3 THE ASX 10 PRINCIPLES[7]

The Australian Stock Exchange (ASX) Corporate Governance Council created ten principles of good governance, including best practices for each. What follows is a summary of the principles and best practices to achieve them.



Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi Massimo, ''Governance Matters V: Governance indicators for 1996–2006'' (July 2007).

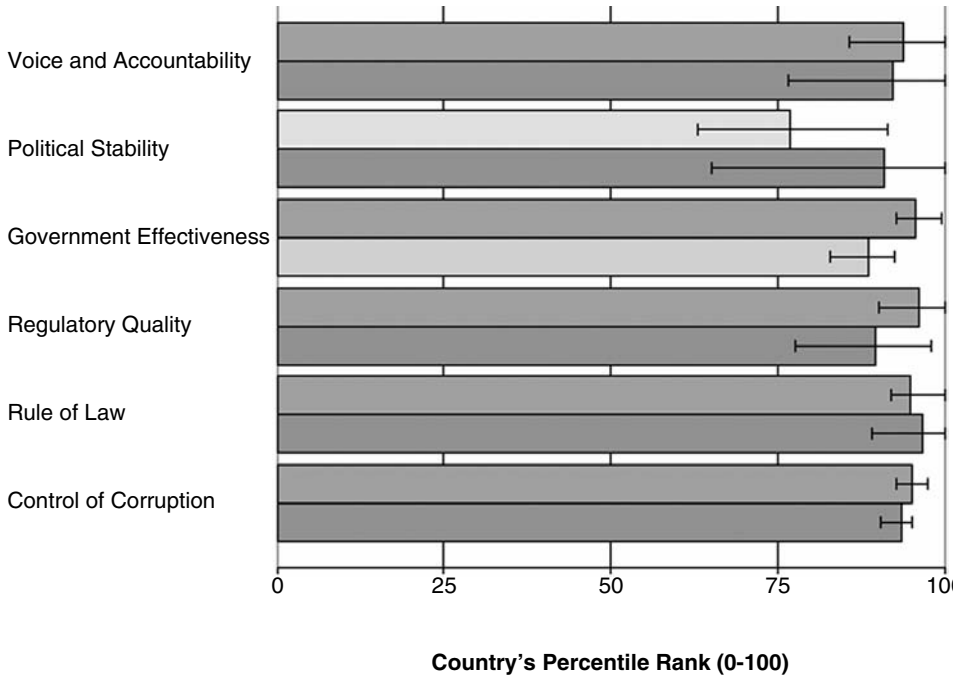
EXHIBIT 49.1(b) RULE OF LAW 2006—AUSTRALIA AND ITS NEIGHBORS



Individual Indicators used to construct Government Effectiveness

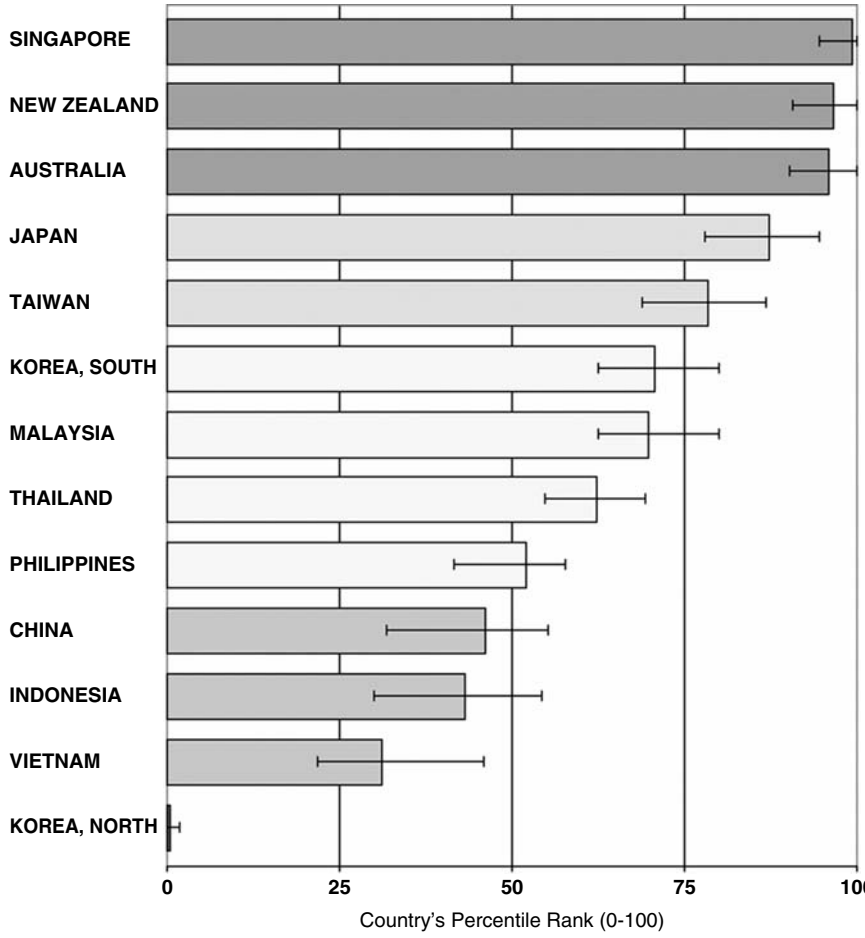
Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi Massimo, ''Governance Matters V: Governance indicators for 1996–2006'' (July 2007).

EXHIBIT 49.1(C) AUSTRALIA, 1996–2006 AGGREGATE INDICATOR: GOVERNMENT EFFECTIVENESS CONSISTENTLY HIGH FOR 10 YEARS



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

EXHIBIT 49.2 WORLD BANK GOVERNANCE RANKINGS: SIX ELEMENTS FOR AUSTRALIA 2006 AND 1996 (TOP-TO-BOTTOM ORDER)



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

EXHIBIT 49.3 WORLD BANK GOVERNANCE RANKINGS: REGULATORY QUALITY FOR AUSTRALIA AND SELECTED ASIAN COUNTRIES

(a) PRINCIPLE 1: LAY SOLID FOUNDATIONS FOR MANAGEMENT AND OVERSIGHT. "Recognize and publish the respective roles and responsibilities of board and management." The company's framework should be designed to:

- Enable the board to provide strategic guidance for the company and effective oversight of management
- Clarify the respective roles and responsibilities of board members and senior executives in order to facilitate board and management accountability to both the company and its shareholders
- Ensure a balance of authority so that no single individual has unfettered powers

Recommendation 1.1. Formalize and disclose the functions reserved to the board and those delegated to management.[8]

Role of the board and management. It is suggested that the board adopt a formal statement of matters reserved to it or a formal board charter that details the functions and responsibilities of the board. Another alternative is a formal statement of delegated authority to management. The nature of matters reserved to the board and delegated to management will necessarily depend on the size, complexity, and ownership structure of the company, and will be influenced by its tradition and corporate culture, and by the skills of directors and managers. Disclosing the division of responsibility assists those affected by corporate decisions to better understand the respective accountabilities and contributions of board and management of the particular company. That understanding can be further enhanced if the disclosure includes an explanation of the balance of responsibility between the chairperson, the lead independent director (if any), and the chief executive officer (or equivalent). The division of responsibility may vary with the evolution of the company. Regular review of the balance of responsibilities may be appropriate to ensure that the division of functions remains appropriate to the needs of the company.

Responsibilities of the board. Usually the board would be responsible for:

- Having oversight of the company, including its control and accountability systems
- Appointing and removing the chief executive officer (or equivalent)
- Ratifying the appointment and, where appropriate, the removal of the chief financial officer (or equivalent) and the company secretary
- Inputting into and final approval of management's development of corporate strategy and performance objectives
- Reviewing and ratifying systems of risk management and internal compliance and control, codes of conduct, and legal compliance
- Monitoring senior management's performance and implementation of strategy, and ensuring appropriate resources are available
- Approving and monitoring the progress of major capital expenditure, capital management, and acquisitions and divestitures
- Approving and monitoring financial and other reporting

Allocation of individual responsibilities. It is also appropriate that directors clearly understand corporate expectations of them. To that end, formal letters of appointment for directors setting out the key terms and conditions relative to that appointment are very useful.

(b) PRINCIPLE 2: STRUCTURE THE BOARD TO ADD VALUE. Have a board of an effective composition, size, and commitment to adequately discharge its responsibilities and duties adequately. An effective board is one that facilitates the efficient discharge of the duties imposed by law on the directors and adds

value in the context of the particular company's circumstances. This requires that the board be structured in such a way that it:

- Has a proper understanding of, and competence to deal with, the current and emerging issues of the business
- Can effectively review and challenge the performance of management and exercise independent judgment

Ultimately, the directors are elected by the shareholders. However, the board and its delegates play an important role in the selection of candidates for shareholder vote.

Recommendation 2.1. A majority of the board should be independent directors.

Assessment of independence. An independent director is independent of management and free of any business or other relationship that could materially interfere with—or could reasonably be perceived to materially interfere with the exercise of their unfettered and independent judgment.

Disclosure of independence. The board should regularly assess the independence of each director in light of interests disclosed by them. So that it can do this, each independent director should provide to the board all relevant information. Directors considered by the board to be independent should be identified as such in the corporate governance section of the annual report. The board should state its reasons if it considers a director to be independent notwithstanding the existence of relationships. In this context, it is important for the board to must consider materiality thresholds from the perspective of both the company and its directors, and to disclose these. The tenure of each director is important to an assessment of independence. The board should disclose the period of office of each director in the corporate governance section of the annual report. Where the independent status of a director is lost, this should be immediately disclosed to the market.

Independent decision making. All directors should bring an independent judgment to bear in decision making. To facilitate this, there should be a procedure agreed by the board for directors to take independent professional advice if necessary, at the company's expense. Nonexecutive directors should consider the benefits of conferring regularly at scheduled sessions without management present. Their discussions can be facilitated by the chairperson or lead independent director. Family ties and cross-directorships may be relevant in considering interests and relationships that may compromise independence, and should be disclosed by directors to the board.

Recommendation 2.2. The chairperson should be an independent director.

Role of chairperson. The chairperson is responsible for leadership of the board, for the efficient organization and conduct of the board's function, and for the briefing of all directors in relation to issues arising at board meetings. It is important that the chairperson must facilitate the effective contribution of

all directors and promote constructive and respectful relations between board members and between board and management. Where the chairperson is not an independent director, it may be beneficial to consider the appointment of a lead independent director. It is vital that the chairperson must commit the time necessary to discharge that role effectively. In that context, the number of other positions, and time commitment associated with them, should be taken into account.

Recommendation 2.3. The roles of chairperson and chief executive officer should not be exercised by the same individual.

There needs to be a clear division of responsibility at the head of the company. The division of responsibilities between the chairperson and the chief executive officer should be agreed by the board and set out in a statement of position authority. The chief executive officer (CEO) should not go on to become chairperson of the same company.

Recommendation 2.4. The board should establish a nomination committee.

Purpose of the nomination committee. Particularly in larger companies, a nomination committee can be a more efficient mechanism for the detailed examination of selection and appointment practices meeting the needs of the company. The existence of a nomination committee should not be seen as implying a fragmentation or diminution of the responsibilities of the board as a whole. It is recognized that for smaller boards, the same efficiencies may not be apparent from a formal committee structure.

Composition of nomination committee. The nomination committee should consist of a minimum of three members, the majority being independent directors and be chaired by the chairperson of the board or an independent director.

Charter. The nomination committee should have a charter that clearly sets out clarifies its role and responsibilities, composition, and structure and membership requirements.

Responsibilities. Responsibilities of the committee should include:

- Assessment of the necessary and desirable competencies of board members
- Review of board succession plans
- Evaluation of the board's performance
- Recommendations for the appointment and removal of directors

Selection process. A formal and transparent procedure for the selection and appointment of new directors to the board helps promote investor understanding and confidence in that process.

Director competencies. Corporate performance is enhanced when there is a board with the appropriate competencies to enable it to discharge its mandate effectively. An evaluation of the range of skills, experience, and expertise on the board is, therefore, beneficial before a candidate is recommended for appointment. Such an evaluation enables identification of the particular skills, experience, and expertise that will best complement board effectiveness. The nomination committee should consider developing and implementing a plan for identifying, assessing,

and enhancing director competencies. The nomination committee should also consider whether succession plans are in place to maintain an appropriate balance of skills, experience, and expertise on the board.

Composition and commitment. It is important that the board must be of a size and composition that is conducive to making decisions expediently, with the benefit of a variety of various perspectives and skills, and in the best interests of the company as a whole rather than of individual shareholders or interest groups. The size of the board should be limited so as to encourage efficient decision making. It is also important that individual board members must devote the necessary time to the important tasks entrusted to them. In this context, all directors should consider the number and nature of their directorships and calls on their time from other commitments. In support of their candidature for directorship, nonexecutive directors should provide the nomination committee with details of other commitments and an indication of time involved. Nonexecutive directors should specifically acknowledge to the company prior to appointment or being submitted for election that they will have sufficient time to meet what is expected of them. The nomination committee should regularly review the time required from a nonexecutive director, and whether directors are meeting this. A nonexecutive director should inform the chairperson and the nomination committee before accepting any new appointments.

Election of directors. The names of candidates submitted for election as director should be accompanied by the following information to enable shareholders to make an informed decision on their election:

- Biographical details, including competencies and qualifications and information sufficient to enable an assessment of the independence of the candidate
- Details of relationships between the candidate and the company, the candidate and directors of the company, directorships held, particulars of other positions that involve significant time commitments, the term of office currently served by any directors subject to reelection, and any other particulars required by law

Term of directorship. Nonexecutive directors should be appointed for specific terms subject to reelection and to the ASX Listing Rules and ASX Corporations Act provisions concerning removal of a director. Reappointment of directors should not be automatic.

Recommendation 2.5. Provide the information indicated in the guide to reporting on Principle 2.

The following material should be included in the corporate governance section of the annual report:

- The skills, experience, and expertise relevant to the position of director held by each director in office at the date of the annual report

- The names of the directors considered by the board to constitute independent directors and the company's materiality thresholds
- A statement as to whether there is a procedure agreed by the board for directors to take independent professional advice at the expense of the company
- The term of office held by each director in office at the date of the annual report
- The names of members of the nomination committee and their attendance at meetings of the committee
- An explanation of any departures from best practice recommendations

The following material should be made publicly available, ideally by posting it to the company's web site in a clearly marked corporate governance section:

- A description of the procedure for the selection and appointment of new directors to the board
- The charter of the nomination committee or a summary of the role, rights, responsibilities, and membership requirements for that committee
- The nomination committee's policy for the appointment of directors

Application of Principle 2 in relation to trusts. References to "board" and "directors" should be applied as references to the board and directors of the responsible entity of the trust. There may be a technical conflict in implementing the recommendations that the chairperson be an independent director or a lead independent director, where the responsible entity is a wholly owned subsidiary of a fund manager and all the directors are employees of the parent. This should be discussed and clarified in any explanation of departure from the best practice recommendations included in the corporate governance section of the annual report. Refer also to section 601 JA(2) of the ASX Corporations Act, which sets out the criteria for independence of a director of a responsible entity.

(c) PRINCIPLE 3: PROMOTE ETHICAL AND RESPONSIBLE DECISION MAKING. Actively promote ethical and responsible decision making. The company should:

- Clarify the standards of ethical behavior required of company directors and key executives (i.e., officers and employees who have the opportunity to materially influence the integrity, strategy, and operation of the business and its financial performance) and encourage the observance of those standards
- Publish its position concerning the issue of board and employee trading in company securities and in associated products that operate to limit the economic risk of those securities

Recommendation 3.1. Establish a code of conduct to guide the directors, the chief executive officer (CEO) (or equivalent), the chief financial officer (CFO)

(or equivalent) and any other key executives as to: 3.1.1 (the practices necessary to maintain confidence in the company's integrity), and 3.1.2 (the responsibility and accountability of individuals for reporting and investigating reports of unethical practices).

Good corporate governance ultimately requires people of integrity. Personal integrity cannot be regulated. However, investor confidence can be enhanced if the company clearly articulates the practices by which it intends directors and key executives to abide. Each company should determine its own policies designed to influence appropriate behavior by directors and key executives. A code of conduct is an effective way to guide the behavior of directors and key executives and demonstrate the commitment of the company to ethical practices. It is not necessary to adopt a separate code for directors and key executives.

Principle 10 also recommends corporate codes of conduct. Depending on the nature and size of the company's operations, the code of conduct for directors and key executives may stand alone or be part of the corporate code of conduct recommended in Principle 10.

Recommendation 3.2. Disclose the policy concerning trading in company securities by directors, officers, and employees.[9]

Public confidence in the company can be eroded if there is insufficient understanding about the company's policies governing trading by potential insiders. The law prohibits insider trading, and the ASX Corporations Act and the ASX Listing Rules require disclosure of any trading undertaken by directors or their related entities in the company's securities. In the interests of investor confidence, companies should consider complementing these requirements with a formal policy governing trading practices. For the purpose of this policy a "potential insider" is a person likely to possess inside information and includes the directors, the chief executive officer (or equivalent), the chief financial officer (or equivalent), staff members who are involved in material transactions concerning the company, and any other member of staff who is likely to be in the possession of inside information. Inside information is information concerning the company's financial position, strategy, or operations, which, if made public, would be likely to have a material impact on the price of the company's securities.

(d) PRINCIPLE 4: SAFEGUARD INTEGRITY IN FINANCIAL REPORTING. Have a structure to independently verify and safeguard the integrity of the company's financial reporting. This requires the company to put in place a structure of review and authorization designed to ensure the truthful and factual presentation of the company's financial position. For example, the structure would include, for example:

- Review and consideration of the accounts by the audit committee
- A process to ensure the independence and competence of the company's external auditors

Such a structure does not diminish the ultimate responsibility of the board to ensure the integrity of the company's financial reporting.

Recommendation 4.1. Require the chief executive officer (CEO) (or equivalent) and the chief financial officer (CFO) (or equivalent) to state in writing to the board that the company's financial reports present a true and fair view, in all material respects, of the company's financial condition and operational results and are in accordance with relevant accounting standards.

Interaction with ASX Corporations Act. The requirement to make this statement encourages management accountability and provides an underpinning for the statements required by the directors under the ASX Corporations Act in relation to the company's financial reports.

Recommendation 4.2. The board should establish an audit committee.

Purpose of the audit committee. Particularly for larger companies, an audit committee can be a more efficient mechanism than the full board for focusing the company on particular issues relevant to verifying and safeguarding the integrity of the company's financial reporting. The existence of an audit committee should not be seen as implying a fragmentation or diminution of the responsibilities of the board as a whole. It is recognized that for smaller boards, the same efficiencies may not be apparent from a formal committee structure.

Importance of the audit committee. The existence of an independent audit committee is recognized internationally as an important feature of good corporate governance. If there is no audit committee, it is particularly important that the company disclose how its alternative approach assures the integrity of the financial statements of the company and the independence of the external auditor, and why an audit committee is not considered appropriate.

Recommendation 4.3. Structure the audit committee so that it consists of:

- Only nonexecutive directors
- A majority of independent directors
- An independent chairperson who is not chairperson of the board
- At least three members

The audit committee should be of sufficient size, independence, and technical expertise to discharge its mandate effectively.

Importance of independence. The ability of the audit committee to exercise independent judgment is vital. International best practice is moving towards an audit committee comprised of only independent directors. The ASX Corporate Governance Council encourages companies to move toward such a composition within the next three years and will be monitoring audit committee composition and international developments in this area.

Technical expertise. The audit committee should include members who are all financially literate (i.e., are able to read and understand financial statements);

have at least one member who has financial expertise (i.e., is a qualified accountant or other financial professional with experience of financial and accounting matters); and contain some members who have an understanding of the industry in which the entity operates.

Recommendation 4.4. The audit committee should have a formal charter.[10]

Charter. The charter should clearly set out the audit committee's role and responsibilities, composition, structure, and membership requirements. The audit committee should be given the necessary power and resources to meet its charter. This will include rights of access to management and to auditors (external and internal) without management present and rights to seek explanations and additional information.

Responsibilities. The audit committee should review the integrity of the company's financial reporting and oversee the independence of the external auditors.

Meetings. The audit committee should meet often enough to undertake its role effectively. The audit committee should keep minutes of its meetings and these should ordinarily be included in the papers for the next full board meeting after each audit committee meeting.

Reporting. The audit committee should report to the board. The report should contain all matters relevant to the committee's role and responsibilities, including:

- Assessment of whether external reporting is consistent with committee members' information and knowledge and is adequate for shareholder needs
- Assessment of the management processes supporting external reporting
- Procedures for the selection and appointment of the external auditor and for the rotation of external audit engagement partners
- Recommendations for the appointment or removal of an auditor
- Assessment of the performance and independence of the external auditors and whether the audit committee is satisfied that independence of this function has been maintained having regard to the provision of nonaudit services
- Assessment of the performance and objectivity of the internal audit function
- The results of its review of risk management and internal compliance and control systems

Recommendation 4.5. Provide the information indicated in the guide to reporting on Principle 4.

Guide to reporting on Principle 4. The following material should be included in the corporate governance section of the annual report:

- Details of the names and qualifications of those appointed to the audit committee, or, where an audit committee has not been formed, those who fulfill the functions of an audit committee

- The number of meetings of the audit committee and the names of the attendees
- Explanation of any departures from best practice recommendations

The following material should be made publicly available, ideally by posting it to the company's web site in a clearly marked corporate governance section:

- The audit committee charter
- Information on procedures for the selection and appointment of the external auditor, and for the rotation of external audit engagement partners

(e) PRINCIPLE 5: MAKE TIMELY AND BALANCED DISCLOSURE. Promote timely and balanced disclosure of all material matters concerning the company. This means that the company must put in place mechanisms designed to ensure compliance with the ASX Listing Rules requirements such that:

- All investors have equal and timely access to material information concerning the company—including its financial situation, performance, ownership, and governance.
- Company announcements are factual and presented in a clear and balanced way.

Balance requires disclosure of both positive and negative information.

Recommendation 5.1. Establish written policies and procedures designed to ensure compliance with ASX Listing Rules disclosure requirements and to ensure accountability at a senior management level for that compliance.

There should be vetting and authorization processes designed to ensure that company announcements:

- Are made in a timely manner
- Are factual
- Do not omit material information
- Are expressed in a clear and objective manner that allows investors to assess the impact of the information when making investment decisions

Recommendation 5.2. Provide the information indicated in the guide to reporting on Principle 5.

The following material should be included in the corporate governance section of the annual report: an explanation of any departures from best practice recommendation.

The following material should be made publicly available, ideally by posting it to the company's web site in a clearly marked corporate governance section: a summary of the policies and procedures designed to guide compliance with ASX Listing Rules disclosure requirements.

(f) PRINCIPLE 6: RESPECT THE RIGHTS OF SHAREHOLDERS. Respect the rights of shareholders and facilitate the effective exercise of those rights. This means that a company should empower its shareholders by:

- Communicating effectively with them
- Giving them ready access to balanced and understandable information about the company and corporate proposals
- Making it easy for them to participate in general meetings

Recommendation 6.1. Design and disclose a communications strategy to promote effective communication with shareholders and encourage effective participation at general meetings. Publishing the company's policy on shareholder communication will help investors to access the information.

Electronic communication. Companies should consider how best to take advantage wherever practicable of new technologies that provide:

- Greater opportunities for more effective communications with shareholders
- Improved access for shareholders unable to be physically present at meetings

Meetings. Consider how to use general meetings effectively to communicate with shareholders and allow reasonable opportunity for informed shareholder participation.

Communication with beneficial owners. Companies may wish to consider allowing beneficial owners to choose to receive shareholder materials directly—for example, by electronic means.

Web site. Companies are encouraged, but not required, to maintain a company web site, and to communicate with shareholders via electronic methods. If the company does not have a web site, it must make relevant information available to shareholders by other means; for example, a company may provide the information on request by e-mail, fax, or postal mail.

Recommendation 6.2. Request the external auditor to attend the annual general meeting and be available to answer shareholder questions about the conduct of the audit and the preparation and content of the auditor's report.

(g) PRINCIPLE 7: RECOGNIZE AND MANAGE RISK. Establish a sound system of risk oversight and management and of internal control. This system should be designed to identify, assess, monitor, and manage risk, and to inform investors of material changes to the company's risk profile. This structure can enhance the environment for identifying and capitalizing on opportunities to create value.

Recommendation 7.1. The board or appropriate board committee should establish policies on risk oversight and management.

Purpose of the committee. Particularly for larger companies, a committee can be a more efficient mechanism than the full board for focusing the company

on risk oversight and management and on internal control. The appropriate board committee may be the audit committee, the risk management committee, or some other relevant committee. The existence of a committee should not be seen as implying a fragmentation or diminution of the responsibilities of the board as a whole. It is recognized that for smaller boards, the same efficiencies may not be apparent from a formal committee structure.

Policies. The policies should clearly describe the roles and respective accountabilities of the board, audit committee (or other appropriate board committee), management and any internal audit function. They should include the following components: oversight, risk profile, risk management, compliance and control, and assessment of effectiveness.

Oversight of the risk management system. It is part of the board's oversight role to oversee the establishment and implementation of the risk management system, and to review at least annually the effectiveness of the company's implementation of that system.

Risk profile. The risk profile should be a description of the material risks facing the company. Material risks include financial and nonfinancial matters. The risk profile should be regularly reviewed and updated.

Risk management and compliance and control. Management should establish and implement a system for identifying, assessing, monitoring, and managing material risk throughout the organization. This system will include the company's internal compliance and control systems.

Assessment of effectiveness. A company will require some means of analyzing the effectiveness of its risk management and internal compliance and control system and of the effectiveness of its implementation. This will generally be undertaken by the internal audit function, but an alternative mechanism may be employed to achieve the same outcome, depending on the company's size and complexity and the types of risk encountered.

A company, particularly a substantial company, is encouraged to have an internal audit function.

Internal audit function. The audit committee should recommend to the board the appointment and dismissal of any chief internal audit executive. The internal audit function should be independent of the external auditor. The internal audit function should report to management and should have all necessary access to management and the right to seek information and explanations. The audit committee should oversee the scope of the internal audit and should have access to the internal audit function without the presence of management. In order to enhance the objectivity and performance of the internal audit function, companies should consider a second reporting line from the internal audit function to the board or relevant committee.

Recommendation 7.2. The chief executive officer (CEO) (or equivalent) and the chief financial officer (CFO) (or equivalent) should state to the board in writing that: the statement given in accordance with best practice recommendation

4.1 (the integrity of financial statements) is founded on a sound system of risk management and internal compliance and control, which implements the policies adopted by the board, and that the company's risk management and internal compliance and control system is operating efficiently and effectively in all material respects. The integrity of the company's financial reporting depends on the existence of a sound system of risk oversight and management and internal control. The requirement to make this statement encourages management accountability in this area.

Recommendation 7.3. Provide the information indicated in the guide to reporting on Principle 7.

Guide to reporting on Principle 7. The following material should be included in the corporate governance section of the annual report: explanation of any departures from best practice recommendations.

The following material should be made publicly available, ideally by posting it to the company's web site in a clearly marked corporate governance section: a description of the company's risk management policy and internal compliance and control system.

(h) PRINCIPLE 8: ENCOURAGE ENHANCED PERFORMANCE. Fairly review and actively encourage enhanced board and management effectiveness. This means that directors and key executives should be equipped with the knowledge and information they need to discharge their responsibilities effectively, and that individual and collective performance is regularly and fairly reviewed. How to achieve best practice:

Recommendation 8.1. Disclose the process for performance evaluation of the board, its committees and individual directors, and key executives.

Performance review. The performance of the board and key executives should be reviewed regularly against both measurable and qualitative indicators. The nomination committee should take responsibility for evaluating the board's performance.

Facilitating performance by education. The company should implement induction procedures designed to allow new board appointees to participate fully and actively in board decision making at the earliest opportunity. New directors cannot be effective until they have a good deal of knowledge about the company and the industry within which it operates. An induction program should be made available that enables directors to gain an understanding of:

- The company's financial, strategic, operational, and risk management position
- Their rights, duties, and responsibilities
- The role of the board committees

The nomination committee should be responsible for ensuring that an effective induction process is in place, and should regularly review its effectiveness.

Similar induction processes may also be desirable for key executives. Directors and key executives should have access to continuing education to update and enhance their skills and knowledge. This should include education concerning key developments in the company and within the industry and environments within which it operates.

Access to information. The board should be provided with the information it needs to efficiently discharge its responsibilities efficiently. In particular, it is important that:

- There must be a procedure agreed by the board for directors to take independent professional advice if necessary, at the company's expense.
- All directors must have access to the company secretary.
- The appointment and removal of the company secretary must be a matter for decision by the board as a whole.

Management should supply the board with information in a form, time frame, and quality that will enable the board to effectively discharge its duties effectively. Directors should be entitled to, and prepared to request, additional information where they consider that the information supplied by management is insufficient to support informed decision making.

The company secretary plays an important role in supporting the effectiveness of the board by monitoring that board policy and procedures are followed, and in coordinating the completion and dispatch of board agenda and briefing materials. The company secretary should be accountable to the board, through the chairperson, on all governance matters.

(i) PRINCIPLE 9: REMUNERATE FAIRLY AND RESPONSIBLY. Ensure that the level and composition of remuneration is sufficient and reasonable and that its relationship to corporate and individual performance is defined. This means that companies need to adopt remuneration policies that attract and maintain talented and motivated directors and employees so as to encourage enhanced company performance of the company. It is important that there must be a clear relationship between performance and remuneration, and that investors must understand the policy underlying executive remuneration be understood by investors. How to achieve best practice:

Recommendation 9.1. Provide disclosure in relation to the company's remuneration policies to enable investors to understand the costs and benefits of those policies and the link between remuneration paid to directors and key executives and corporate performance.

Reporting. Disclosing the remuneration policy is a fundamental requirement for remuneration reporting. The interests of shareholders and the market are best served through a transparent and readily understandable framework for executive compensation and its costs and benefits. Transparency as to the remuneration policy should be complemented by full and effective disclosure, in keeping with

the spirit and intent of the ASX Corporations Act and the ASX Listing Rules, of the remuneration paid to directors and senior management.

Annual disclosure. The ASX Corporations Act requires annual disclosure by a listed company of the details of the nature and amount of each element of the fee or salary of each director and each of the five highest-paid officers of the company. This includes disclosure in respect of nonmonetary components, such as options. Disclosure should focus on the remuneration components that are related to continuing employment with the company or other companies in the same group. Accordingly, if an executive has been terminated during the year and the termination and other benefits paid classify that executive as one of the five highest-paid executives, the relevant disclosure should include the five highest-paid executives continuing in employment. Any loans to executives and directors (other than those made on commercial terms) should be included with this disclosure, including the amount and the interest rate. Benefits such as motor vehicles, rent, travel and relocation allowances, and other benefits should also be included. Effective disclosure requires valuing the various components and describing the valuation techniques used.

Continuous disclosure. Entering employment agreements with key executives, or obligations under these agreements falling due, may trigger a continuous disclosure obligation under ASX Listing Rule 3.1. Where this is the case, disclosure to the market should include a summary of the main elements and terms of the agreement, including termination entitlements. In considering the appropriate matters for disclosure to the market and fostering a constructive relationship with shareholders, the sensitivities of significant payments to key executives should be considered.

Improving corporate behavior. Australia needs a framework for disclosure that will produce sustainable improvements in corporate behavior concerning remuneration practices. The issues associated with the establishment of such a framework are complex. The right framework requires:

- Clarification of the disclosure policy and requirements of the ASX Corporations Act relative to matters such as the value of stock options and disclosure of accruals of termination and other payments
- Complementary Australian Accounting Standards Board (AASB) standards, including finalization of the proposed AASB standard on director, executive, and related-party disclosures
- A careful balance in the amount and type of disclosure, so that its outcome is relevant information to investors, and not simply enhanced market conditions for increasing levels of individual remuneration to the detriment of shareholders

The enhanced framework for determining, reviewing, and reporting on remuneration of directors and executives outlined in this document is a significant

step in improving the information available to investors and influencing corporate behavior. However, the ASX Corporate Governance Council has agreed as a matter of priority to examine the need for additional disclosure, including for a wider range of executives. The ASX Corporate Governance Council encourages companies to restore investor confidence by adopting disclosure practices designed to enhance awareness of key aspects of the remuneration framework and its link to performance.

Eliminating surprise. Shareholder concern about executive payments is often exacerbated by a lack of information concerning core entitlements when they are agreed on. This can be alleviated if, for example, the nature of the termination entitlements of the chief executive officer (CEO) (or equivalent) is disclosed to the market at the time they are agreed on as well as at the time the actual payment is settled.

Recommendation 9.2. The board should establish a remuneration committee.

Purpose of the remuneration committee. Particularly for larger companies, a remuneration committee can be a more efficient mechanism than the full board for focusing the company on appropriate remuneration policies that are designed to meet the needs of the company and to enhance corporate and individual performance. The existence of a remuneration committee should not be seen as implying a fragmentation or diminution of the responsibilities of the board as a whole. It is recognized that for smaller boards, the same efficiencies may not be apparent from a formal committee structure.

Composition of remuneration committee. The remuneration committee should:

- Consist of a minimum of three members, the majority being independent directors
- Be chaired by an independent director

Charter. The remuneration committee should have a formal charter that clearly sets out its role and responsibilities, composition, structure, and membership requirements.

Responsibilities. The responsibilities of the remuneration committee should include a review of and recommendation to the board on:

- Executive remuneration and incentive policies
- The remuneration packages of senior management
- The company's recruitment, retention, and termination policies
- Procedures for senior management
- Incentive schemes
- Superannuation arrangements
- The remuneration framework for directors

Remuneration policies. The company should design its remuneration policy in such a way that it motivates directors and management to pursue the

long-term growth and success of the company within an appropriate control framework, and it demonstrates a clear relationship between key executive performance and remuneration. The remuneration framework for directors is often addressed by the nomination committee rather than the remuneration committee. The remuneration committee may seek input from individuals on remuneration policies, but no individuals should not be directly involved in deciding their remuneration. The remuneration committee should ensure that the board, management, and the remuneration committee are provided with sufficient information to ensure informed decision making. Executive remuneration packages should involve a balance between fixed and incentive pay, reflecting short-term and long-term performance objectives appropriate to the company's circumstances and goals. A proportion of executive directors' remuneration should be structured in a manner designed to link rewards to corporate and individual performance.

Recommendation 9.3. Clearly distinguish the structure of nonexecutive directors' remuneration from that of executives.

Where schemes for retirement benefits for nonexecutive directors are in place, their existence and terms should be clearly disclosed in the corporate governance section of the annual report, including the provision accrued each year together with the total amount accrued to date. The relevant amount should be disclosed as a component of each participating director's remuneration.

Recommendation 9.4. Ensure that payment of equity-based executive remunerations made in accordance with thresholds set in plans approved by shareholders.

Recommendation 9.5. Provide the information indicated in the guide to reporting on Principle 9.

(j) PRINCIPLE 10: RECOGNIZE THE LEGITIMATE INTERESTS OF STAKEHOLDERS[11]. Recognize legal and other obligations to all legitimate stakeholders. Companies have a number of legal and other obligations to nonshareholder stakeholders, such as employees, clients/customers, and the community as a whole. There is growing acceptance of the view that organizations can create value by better managing natural, human, social, and other forms of capital. Increasingly, the performance of companies is being scrutinized from a perspective that recognizes these other forms of capital. That being the case, it is important for companies to demonstrate their commitment to appropriate corporate practices.

Recommendation 10.1. Establish and disclose a code of conduct to guide compliance with legal and other obligations to legitimate stakeholders.

Most companies are subject to a number of legal requirements that affect the way business is conducted. These include trade practices and fair dealing laws, consumer protection, respect for privacy, employment law, occupational health and safety, equal employment opportunity, superannuation, and environmental and pollution controls. In several areas, directors and officers are held personally responsible for corporate behavior inconsistent with these requirements, and

penalties can be severe. Aside from the need to effectively manage risk effectively and support compliance with the company's legal obligations, there is the broader issue of enhancement of corporate reputation. In this context, consultation with the governments and communities in whose territory business is conducted is important. Public or social accountability by corporations is generally based on notions of legitimacy, fairness, and ethics. The board has a responsibility to set the tone and standards of the company and to oversee adherence to these. Company codes of conduct that state the values and policies of the company can assist the board in this task and complement the company's risk management practices.

Corporate code of conduct. Codes of conduct should address matters relevant to the company's compliance with its legal obligations to stakeholders. A code of conduct should enable employees to alert management and the board in good faith to potential misconduct without fear of retribution, and should require recording and investigation of such alerts. The company should have a system for ensuring compliance with its code of conduct and for dealing with complaints. In devising and implementing that system, the laws concerning defamation and privacy need to be considered.

Notes

1. This section extensively references and quotes the Australian Stock Exchange's "ASX Corporate Governance Council Principles of Good Corporate Governance and Best Practice Recommendations," March 2003, www.asx.com.au/corporategovernance.
2. ASX Listing Rule 4.10.3: Introduced 1/7/96. Origin: Listing Rule 3C(3)(e), 3B(2C). Amended 1/7/97, 1/7/98, 1/9/99, 30/9/2001. Cross reference: Listing rules 5.6 and 19.11A.
3. ASX Listing Rule 3.1: Compliance and Policy Rules, Exposure Draft, July 2002.
4. Australian Government, Treasury, Part 10: Enforcement Issues, 2002.
5. World Bank web site: "Comparison within One Country for All Six Governance Indicators," http://info.worldbank.org/governance/kkz2005/sc_country.asp.
6. World Bank web site: "Comparison for One Governance Indicator across a Number of Countries," http://info.worldbank.org/governance/kkz2005/mc_indicator.asp.
7. This section extensively quotes the Code of Conduct for Chief Financial Officers, Group of 100, December 2002. See www.group100.com.au.
8. For further guidance, see C. Smith, N. Milne, and F. Morris, *A Guide to Directors and Officers Liability Insurance* (n.p.: Australian Institute of Company Directors, 2001).
9. For further guidance, see "Code of Conduct for Chief Financial Officers," Group of 100, December 2002, www.group100.com.au. Further guidance may be found at www.csaust.com and at www.companydirectors.com.au. Also, see ASX Listing Rule 3.19A regarding disclosure by the company of directors' modifiable interests within five business days.
10. A detailed guide to the responsibilities of the audit committee is provided in *Best Practice Guide—Audit Committees*, 2nd ed. (n.p.: Auditing and Assurance Standards

Board of the Australian Accounting Research Foundation, Institute of Internal Auditors, Australian Institute of Company Directors, 2001). See www.aarf.asn.au.

11. For further guidance, see Standards Australia web site at www.standards.com.au: "AS3806—Compliance Programs," 1998; "Draft DR03027 (Project ID: 4303)—Organizational Codes of Conduct," 2003; "Draft DR03028 (Project ID: 4304)—Corporate Social Responsibility," 2003; "Draft DR03029 (Project ID: 4305)—Whistleblowing Systems for Organizations," 2003.

CHAPTER 50

CORPORATE GOVERNANCE: INDONESIA

Lawrence Wasserman, PhD

50.1 BACKGROUND

Indonesia is the world's largest archipelagic state and home to the world's largest Muslim population. The nation declared its independence after Japan's surrender in World War II. After four years of intermittent negotiations, recurring hostilities, and UN mediation, the Netherlands agreed to relinquish its colony.

Indonesia is a unitary state, governed by President Sukarno, leader of the national freedom struggle and military dictator, for most of its modern history. Indonesia's first direct presidential election was held in 2004 and won by Susilo Bambang Yudhoyono; it was the largest one-day election in the world.

Although the national language is Indonesian (called Bahasa Indonesia in Indonesian) and the population is overwhelmingly Muslim, there are several hundred diverse linguistic and ethnic groups across the country, as well as other religious communities.

As a country, Indonesia has witnessed political and economic instability during the past two decades or more with President Suharto's abdication and

subsequent malaise of the economy. Democracy was restored following the revolution of 1998.

The Asian economic crisis of the 1990s had long-term implications on Indonesia with a subsequent malaise of the economy. It also had a devastating impact on the nation's private sector participation in the advances in its economy.

Indonesia was the nation hardest hit by the December 2004 tsunami, especially Aceh province with over 100,000 deaths and over $4 billion in damage. An earthquake in March 2005 added to the problem, causing heavy destruction on the island of Nias. The devastated areas may take up to a decade to recover. In 2005, Indonesia reached a historic peace agreement with armed separatists in Aceh, but it continues to face a low-intensity separatist guerilla movement in Papua. Each of these crises had a negative effect on corporate investment in the country.

According to the U.S. Central Intelligence Agency, the country faces the following challenges: alleviating poverty, preventing terrorism, consolidating democracy after four decades of authoritarianism, implementing financial sector reforms, stemming corruption, and holding the military and police accountable for human rights violations.[1]

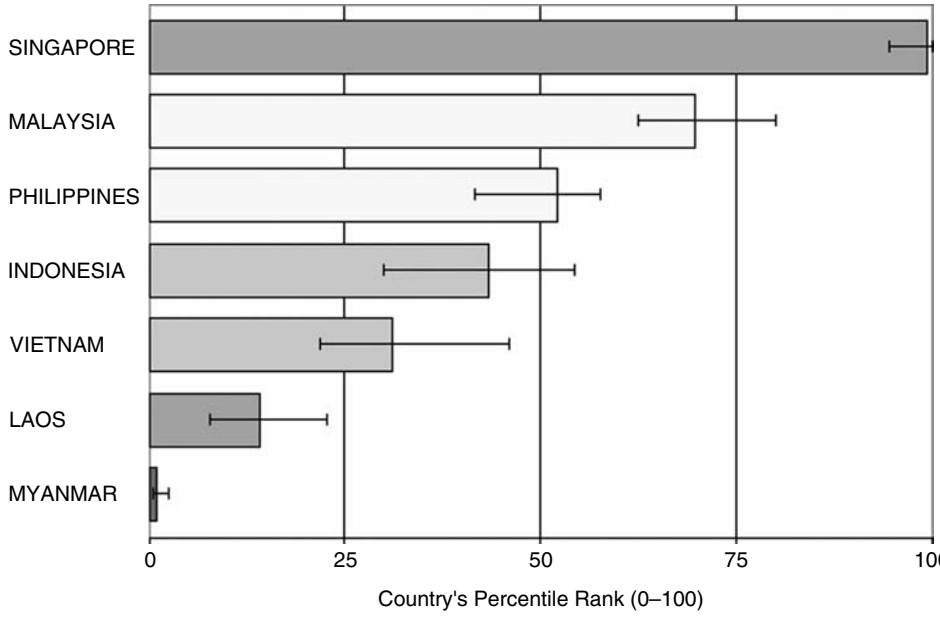
The establishment of the World Trade Organization's open trade movements created a system of free markets among the world countries and had a significant impact on the Asian economy.

One impact was that Indonesia as well as other Asian countries sought private sector investment as a means for its financial markets to maintain their viability and attract foreign investment. A climate of entrepreneurship from government control was needed to enhance national wealth after years of regional stagnation. The growth of Asian countries' economies put pressure on Indonesia to open up its trade policies to world trade.

The corporate crisis in the United States in the 1990s at the executive level (i.e., Enron, WorldCom, etc.) expanded to other worldwide markets of the global economies and financial system. This scandal called for a combination of financial deregulation and control, and the removal of secrecy of activities within companies.

The World Bank rates nations on six areas of governance. By these criteria, Indonesia does not measure up to its Southeast Asian neighbors.[2] It should be noted that countries scoring above Indonesia have higher per capita gross domestic products (GDPs) as measured by purchasing price parity (PPP). Indonesia ranks sixth in two key World Bank indexes of governance and ranks fifth in per capita GDP, according to the CIA's *The World Factbook*. Per capita GDP of selected South East Asian Nations:

Singapore	$28,000	Indonesia	$3,600
Malaysia	$12,000	Vietnam	$2,800
Thailand	$8,000	Laos	$2,000
Philipines	$4,000	Myamar	$1,700



Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

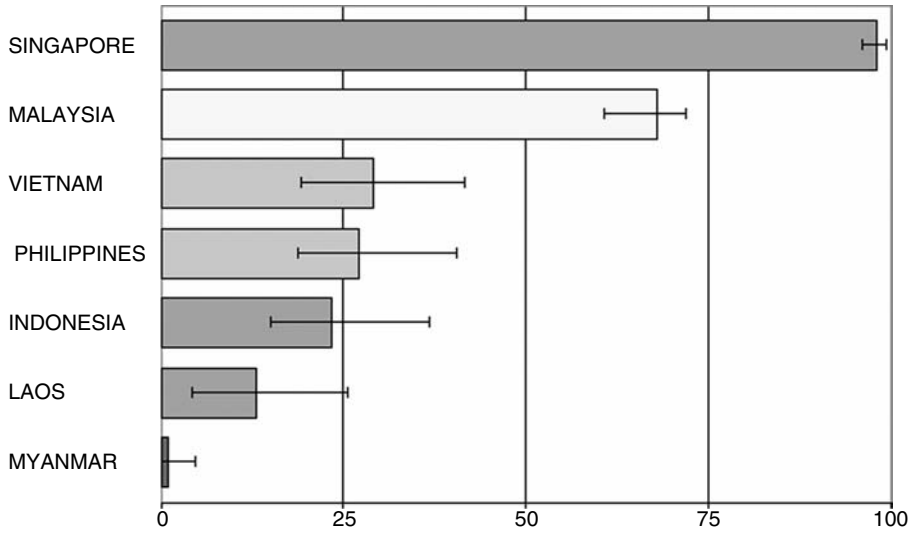
EXHIBIT 50.1 WORLD BANK 2006 GOVERNANCE RANKINGS: REGULATORY QUALITY FOR INDONESIA AND SELECTED S.E. ASIAN COUNTRIES

The World Bank's percentile ranking of governance indicates that Indonesia ranks poorly even by Southeast Asian standards in such critical areas as the role of corruption and regulatory quality (see Exhibit 50.1 and Exhibit 50.2).

As in most Asian countries, the majority of Indonesian companies are controlled by dominant families that pay little attention to the rights of minority investors or the principles of transparency.

Corporate governance regulations have been initiated, which is slowly improving the business climate; however, the Indonesian government has shown no clear legal and legislative reform process.

Indonesia published its national code of best practices on governance in 2001, but separate codes were issued for key sectors of its economy, such as state-owned enterprises in 2002 and the banking industry 2003. In contrast to having national codes, these regulatory improvements appear to have no clear and decisive fundamental change in the way corporate governance is practiced in Indonesia.[3] The Code of Good Corporate Governance was composed by the National Committee on Corporate Governance (NCCG). The objective of the Code is to provide a guide to excellence in corporate governance for the business world that has drawn on international best practice in corporate governance, which appropriately will fit into the Indonesian legal and regulatory environment.



Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 50.2 WORLD BANK 2006 GOVERNANCE RANKINGS: CONTROL OF CORRUPTION FOR INDONESIA AND SELECTED S.E. ASIAN COUNTRIES

The good corporate governance principles as set out in the Code were to be implemented as soon as possible.

Indonesian business needs corporate governance to work in a world economy and requires various instruments to increase its competitiveness. Shareholders' viewpoint is on the need for good corporate governance. Companies that implement good corporate governance, as noted in the Indonesian Code, "in a proper and continuous manner have an advantage over other companies who do not implement or have not implemented good corporate governance."[4]

The Finance Forum Task Force on Macroeconomic Corporate Governance Scorecard of Pacific Economic Cooperation Council (PECC) issued a report where Asia-Pacific Economic Cooperation (APEC) ministers endorsed the PECC guidelines (2001) for good corporate governance practices. The guidelines issued were to promote governance practice in domestic corporations so that they could attract more investment from the international investment community. This project focused on measuring the progress of corporate governance reforms in selected East Asian economies, including Indonesia.

The survey focused on the five corporate governance principles developed by the Organization for Economic Cooperation and Development (OECD). These are the rights of shareholders, equitable treatment of shareholders, role of stakeholders, disclosure and transparency, and board responsibilities. The questionnaire

was based on the authors' selected questions relevant to these economies together with added questions, and the survey was conducted during 2005.

The APEC report focused on applying several corporate governance indexes developed by the international investment community. For example, Standard & Poor's Transparency and Disclosure Index assessed the transparency and disclosure practices of corporations around the world. The Credit Lyonnais Corporate Governance Index applied some major corporate governance factors to rate corporations in different markets. These criteria include discipline, transparency, independence, accountability, responsibility, fairness, and social awareness.

50.2 CORPORATE GOVERNANCE PRACTICES

The Corporate Governance and Financial Reporting Centre (CGFRC) collaborated with Standard & Poor's to examine the corporate governance practices of companies. This joint study on disclosures by the Indonesian LQ45 Index of companies regarding corporate governance practices shows there is much room for improvement.

The study used the corporate governance disclosure scorecard developed by Standard & Poor's to score disclosures of the corporate governance practices of the Indonesian companies. The analysis is based primarily on the disclosures made in the latest annual reports.[5]

The year 2004 saw little substantive progress on the corporate governance front in Indonesia. In terms of the overall country corporate governance score, Indonesia fell slightly, but this was due to a slightly changed questionnaire. While the lack of progress is disappointing, the election of the new president was a milestone for Indonesia. The new president has identified corruption as a major issue for his government, and some progress was reached in his first year. This change, if continued, should lead to improved business practices and has already resulted in the arrest of the president director and two other directors at Bank Mandiri, with a number of other government-run company directors.

With a poor score on the results of macro-determinants for corporate governance, Indonesia was the lowest among the markets surveyed in this report. The score for accounting standards is reasonable and comparable to other markets in the region; but the scores for other categories are generally lower.

The majority of listed Indonesian companies have now instituted audit and remuneration committees, although some look to be relatively powerless. That remains a problem in Indonesia and the region. Companies may be meeting strict legal requirements, but in reality there is little independence in boards and committees and many rely on ex-staff members as independent members.

The legal framework of companies looks reasonably strong, however; but enforcement remains the key issue in Indonesian corporate governance. There have been few, if any, changes in the regulatory environment in the past few

years as to issuing rules. A small number of companies have improved their corporate governance disclosure practices relative to their peers in Indonesia's Q45 Index companies. To summarize the challenges facing Indonesia:

- Only two of the top five companies disclosed the individual attendance of directors and commissioners at their respective meetings.
- None of the top five companies had boards of commissioners with a majority of outside commissioners.
- None of the companies' boards of directors had one-fifth or more outside directors, and none of the companies disclosed whether each director is classified as independent.
- None of the companies disclosed that they had an orientation program for their directors and commissioners when they were appointed to the boards in order to familiarize them with the operations of the company, their legal/fiduciary duties, and expectations. Also, there was no regular training program for directors and commissioners in any of the top five companies.
- Only two of the five companies provided the commissioners with independent access to management and disclosed this fact in the annual report. Only two companies disclosed that they provide the board with separate and independent access to the company secretary.
- No company disclosed that it evaluates the performance of the board of commissioners or individual performance of commissioners. Performance of the board of directors and individual directors was not appraised by any company.
- None of the top five companies disclosed the individual remuneration of commissioners, directors, and the top five executives who were not directors.

A series of reports on corporate governance was produced in collaboration with the Asian Corporate Governance Association (ACGA), an independent nonprofit organization working on behalf of all investors to improve corporate governance practices in Asia.[6] The report has details of the survey, and this section briefly describes the findings, which show little substantive progress in the past few years. Corruption was highlighted as a major issue confronting Indonesia. Major findings include:[7]

Regulatory enforcement: Indonesia's regulatory environment, noted in a report by CG Watch, is fragmented, and the enforcement of these regulations and rules is fragile. Furthermore, securities regulators lack resources and are understaffed and unwilling to undertake vigorous enforcement action. From the viewpoint of the private sector companies, their enforcement is weak and institutional investors timidly exercise their right to vote and rarely attend annual general meetings. Minority shareholders generally are not interested in nominating

independent directors and are unwilling to initiate lawsuits against companies that may be violating regulations. Importantly, Indonesia lacks a reputable independent body to fight endemic corruption.

Political and regulatory environment: 2004 has seen some progress made toward a more open and accountable system of government; however, as noted, Indonesia's political and regulatory institutions remain weak. The Indonesian government lacks the commitment and political will to make lasting and effective reforms in corporate governance, the regulator is not independent of government, and the legal system is especially weak. Minority shareholders do not enjoy cost-effective access to the courts in order to settle disputes, and there is little confidence that the judiciary is capable of handling such disputes in any event. One brighter spot is that Bank Indonesia, the central bank, is becoming increasingly focused on improving the governance of banks.

Accounting and auditing standards: Indonesia, like the rest of the region, has a policy of bringing its accounting standards into line with international ones. Although there is some way to go before its standards align fully with international accounting standards (IAS), current rules do require consolidated accounts, segment reporting (to an extent), and disclosure of connected transactions. Also, there is no requirement for the disclosure of audit and nonaudit fees paid to external auditors. This is significant barrier to meeting corporate governance guidelines.

Cultural and political compliance trends: Indonesian companies are slowly building their own governance cultures at a far lesser extent than in other Asian markets. ACGA's report noted that PT Austindo Nusantara Jaya, a private, unlisted conglomerate, has been voluntarily publishing annual reports since 1994 and has a management team that is clearly aware of governance issues.[8]

Overall, most Indonesian companies pay at best lip service to good governance; the extent of investor activism (at both the institutional and retail level) is extremely limited; and the media do not report on governance abuses as actively as they could.

50.3 CURRENT ENVIRONMENT AND FUTURE TRENDS

The situation remains a problem in Indonesia in that companies may be meeting strict legal requirements but in reality there is little independence in boards and committees. Many rely on ex-staff members as independent members. The Asian Corporate Governance Association provides the following assessment:[9]

- Almost no changes to rules and regulations have been made in the past 12 months. Improvements are stalled.
- There has been little new in the way of enforcement.
- Political and regulatory environment shows signs of drift.

- Indonesian accounting standards/auditing standards generally follow international standards.
- Corporate governance culture in Indonesia remains largely formalistic, with limited evidence of improvements in underlying behavior.[10]

While the legal framework looks reasonably strong, enforcement remains the key issue in Indonesian corporate governance. There have been few, if any, changes in the regulatory environment in 2005. In fact, the English language part of the regulators' web site (www.bapepam.go.id) contains no updates since May 28, 2005. The Indonesian version contains little additional information, although it does include the 2005–2009 Bapepam master plan.

With few changes in the regulatory environment, it has also been a quiet year for companies in terms of corporate governance news. Telkom continues to struggle to meet New York Stock Exchange (NYSE) reporting deadlines (in fact, it is now looking to delist its American depositary receipts [ADRs], which is unlikely to be seen as a positive), but otherwise little has changed.

Among the top corporate governance companies, the Astra Group was well represented. It appears to take corporate governance seriously, which has resulted in strong price performance in recent years. Unilever again takes top spot, despite its limited disclosure. In other ways (responsibility, social, etc.), it is clearly the top company in Indonesia.

The World Bank's "Doing Business" database provides objective measures of business regulations and their enforcement. The database indicators are comparable across 155 national economies, indicating that regulatory costs of business and can be used to analyze specific regulations that enhance or constrain investment, productivity, and growth.

"Doing Business" measures the strength of minority shareholder protections against directors' misuse of corporate assets for personal gain. The indicators distinguish three dimensions of investor protection: The data come from a survey of corporate lawyers and are based on company laws, codes of civil procedure, and securities regulations. Exhibit 50.3 shows the main indicators of investor protection using a one (worst) to ten (best) scale.

One of the latest reports on the assessment of corporate governance in Asia was presented in 2005 by the Asian Corporate Governance Association.[11] The director of the ACGA focused on these four findings:

1. Asian country scores (2005) trended downwards, but not due to a decline in objective corporate governance standards or less effort on the part of regulators.
2. Weaknesses in the detail of laws and regulations have become more apparent.
3. A gap exists between national accounting policies and practices.
4. Corporate governance best practices are not gaining traction among listed companies.[12]

Region or Economy	Disclosure Index	Director Liability Index	Shareholder Suits Index	Investor Protection Index
East Asia & Pacific	5.6	4.2	6.2	5.3
South Asia	4.1	4.6	6.4	5.0
Indonesia	8	5	3	5.3
Malaysia	10	9	7	8.7
Philippines	1	2	7	3.3
Singapore	10	9	9	9.3
Thailand	10	2	6	6.0
Vietnam	4	1	2	2.3

EXHIBIT 50.3 GOVERNANCE INDICATORS: INDONESIA VERSUS OTHER S.E. ASIAN COUNTRIES

(a) INDONESIA FORUM CORPORATE GOVERNANCE INITIATIVES: GOOD GOVERNANCE FRAMEWORK. The Forum for Corporate Governance in Indonesia (FCGI), established in 2000 by five private sector business and professional associations, was very successful in supporting the improvement of corporate governance in dozens of companies.[13]

The main objective of the FCGI is to promote and to foster the implementation of principles and rules of good governance, corporate governance, and corporate sustainability and responsibility (CSR) by companies in Indonesia. The aim is to enhance awareness and to socialize good governance, corporate governance, and CSR principles to the Indonesian business community based on international best practices.

In cooperation with PricewaterhouseCoopers, the Forum issued the fourth edition of the corporate governance booklet updating the latest laws and developments in the corporate governance movement in Indonesia and globally.

In 2002, PricewaterhouseCoopers surveyed international investors to benchmark Indonesia's perceived governance framework relative to other countries in the region.

FCGI's opinion is twofold: (1) Indonesian individual companies, both public and private, bear the main responsibility of observing internationally agreed standards of corporate governance, and (2) companies stand to gain from a system of good corporate governance in advance of stronger enforcement of existing laws and regulations.

(b) FCGI ASSESSMENT OF AND RECOMMENDATIONS FOR INDONESIA GOVERNANCE. The overall assessment of FCGI reports is that Indonesia has taken action in some segments of the economy, enhancing public and foreign confidence in the investment climate. Nevertheless it continues to be eroded by a lack of clarity on policy and the legal environment, and uncertainties regarding the enforcement of the rule of law.

The FCGI reports noted that better alignment of resources and expenditure obligations and greater accountability of public institutions are necessary

to ensure that resources are properly harnessed to construct the physical infrastructure needed for economic growth. An efficient civil service—driven by the right incentives framework, a strong sense of professionalism, and high ethical standards—is indispensable to the implementation of Indonesia's economic and social program agenda.

(i) Asian Development Bank—Assessment of Indonesia Corporate Governance. The Asian Development Bank (ADB) program is committed to support Indonesia in achieving reform. For the past several years, ADB has assisted Indonesia with various programs and projects that aim to foster good governance in one form or another.

The ADB's support includes (1) the governance partnership; (2) initiatives for anticorruption; (3) decentralization programs that aim to develop local government capacities for efficient and effective delivery of services; (4) effective governance through improved accounting, audit, and procurement systems; (5) active policy dialogue and assistance for regional governance policies; and (6) improvement of the state audit function.

This country governance assessment report is a snapshot of the state of governance in Indonesia. It reflects both the achievements and the reform gaps. As such it provides a basis for further dialogue and work on the reform initiatives and their effective management.

The report was prepared drawing upon ADB's extensive economic and sector work, as well as reports from other institutions. It has been extensively discussed with national and regional government institutions and nongovernment stakeholders. This report will encourage Indonesia's citizens, as well as its development partners, to work together with the government in facing and successfully overcoming the many challenges that lie ahead for Indonesia.

(ii) World Bank Corporate Governance Country Assessment Report on the Observance of Standards and Codes, Republic of Indonesia, August 2004[14]. The corporate governance assessment was completed as part of the joint World Bank–International Monetary Fund (IMF) program of Reports on the Observance of Standards and Codes (ROSC). It benchmarks the country's observance of corporate governance against the OECD Principles of Corporate Governance.

The assessment of practices is based on interviews with regulators, institutional investors, financial institutions, market analysts, lawyers, accountants, and auditors, as well as shareholder activists.

Since 2000, Indonesia has taken important steps to address the weaknesses that contributed to the economic crisis of 1997. As a result, the corporate governance framework has been strengthened, but the reform agenda remains unfinished, and the equity markets relative to other East Asian countries remain small.

The ownership structure of companies in Indonesia is characterized by concentrated ownership, family-owned businesses, and controlling shareholders. The business culture is known to be relationship-based rather than rule-based. Most

listed companies are controlled either by families or, in the case of state-owned enterprises, by the government.

In reforming its corporate governance and in establishing a rule-based business culture, Indonesia faces many key challenges; for example, the enforcement of laws and regulations needs to be strengthened. Administrative sanctions for violation of securities or disclosure rules may not be adequate.

The World Bank noted that efforts should be expended to ensure that corporate officials in the position of trust are held accountable when they violate the law. Sanctions should go beyond fines, and the incentive system should be changed so that violators are truly discouraged and good corporate behavior is promoted. This requires strengthening the enforcement capacity of Bapepam (the Indonesian regulatory security agency) for securities violations and its independence as the securities regulator.

The ADB Report assessments can be summarized:

- The Company Law should explicitly refer to the fiduciary duties of directors and managers for violation of securities laws. Current efforts to amend the Company Law need to be expedited.
- Government efforts should also be expended to develop alternative (nonjudiciary) mechanisms, such as shareholder activism, for encouraging compliance. Transparency and reliability of financial reports and adequacy of disclosures remain major challenges as prerequisites to accountability.
- Indonesian accounting standards are largely consistent with international standards; however, there is a gap between those standards and actual practices. The external auditors of public companies in the past have not provided the expected assurance. There is a need for greater disclosure and transparency in annual reports and financial statements, and for better quality audit of public companies.
- The concept of independent commissioners has only recently been introduced for publicly listed companies and state-owned enterprises; there remains the question of whether these commissioners act independently from the controlling shareholders and exercise effective oversight.
- The process for nomination and selection of independent commissioners needs to be strengthened. Conducting training and promoting awareness among all stakeholders are critical to changing the business culture. Efforts to enhance the skills and knowledge of independent board members need to be expedited. Improving the roles and responsibilities of the audit committees should be a high priority.
- Separation of management from the owners and appointment of professional managers need to be further promoted. Further improvements will be required to improve minority shareholder rights and ease with which shareholders exercise those rights. There is a need to further enhance shareholder rights by allowing minority shareholders a greater voice in the

selection of commissioners (i.e., cumulative voting). Additional steps to improve the process for nomination of independent commissioners include requiring establishment of nomination committees.

- While class action and derivative actions are allowed, these are costly and, therefore, have been limited so far to only a few cases and none with a favorable outcome.
- The redress available to shareholders if their rights are violated remains limited. While Indonesia has an elaborate system of formal corporate governance rules, which in several respects may not be substantially different from those of OECD countries, corporate governance practices often fall short of the recommendations of the OECD Principles. The challenge is raising awareness and increasing effectiveness of implementation and enforcement of legislation and regulations to improve the corporate culture and practices.

(iii) Corporate Governance 2002 Report on Institutional Investor Survey Conducted by IICD/IICG[15]. There have been numerous researches/surveys on corporate governance in Indonesia carried out by organizations such as Indonesian Institute of Corporate Governance (IICG) and Indonesian Institute of Corporate Directorship (IICD). Generally, these surveys scored corporate governance practices of publicly listed companies.

An example of assessment of the reform efforts and their effects on corporate governance practices at the corporate level is the relevant corporate governance survey carried out by the Jakarta Stock Exchange (JSX). In 2002, the JSX carried out a survey of senior management and senior investment managers of local entities involved in investment in Indonesian stock markets (collectively referred to as institutional investors), including insurance firms, pension funds, research analysts, and fund managers. The survey was designed to provide an understanding of how institutional investors view corporate governance practices and disclosures in Indonesia in the context of their investment decisions. Three highlighted issues from the survey are:

1. *Factors affecting investment decisions.* Respondents to the survey said that they would be prepared to pay a premium of 17 percent for a company that is perceived to have good governance. In addition, the respondents indicated that economic macro and structural issues (or external factors), such as legal certainty, security concerns, and currency risk are considered to have the biggest influence on investment decisions in Indonesia and have the effect of overshadowing recent improvements in corporate governance.
2. *State of corporate governance in Indonesia.* Fifty percent of the institutional investors felt that there have been improvements in standards of business ethics and corporate governance in Indonesia. According to the survey report, there is a low level of awareness about new initiatives

in Indonesia to improve corporate governance, including the issuance of the National Code of Good Corporate Governance. The survey revealed there is an indication that the institutional investors believe weaker crony relationships will provide a better environment for the improvement of corporate governance. Institutional investors believe that a reduction in "KKN" (corruption, collusion, and nepotism) is of great importance for improving the existing governance practices.

3. *Perceived governance standards compared to other countries in the region.* Indonesian investors believe that corporate governance practices in Indonesia rank alongside other emerging markets, such as the People's Republic of China (PRC), India, and Thailand, and still lag behind those adopted in developed countries. The leaders are still Singapore, Australia, Japan, and Hong Kong. In relation to auditing and compliance, disclosure and transparency, and board processes, Indonesia was perceived to be comparable and in some cases better than other emerging nations in the survey. However, there was concern about perceived standards of accountability to shareholders. This may reflect in part the wider macro conditions of a weak legal system, which are beyond the control of listed companies or their regulators.

(A) Country Governance Assessment Report, Republic of Indonesia, ADB, 2004[16]

ADB conducted a Country Governance Assessment Report as a snapshot of the state of governance in Indonesia. It reflects both the achievements and the reform gaps. It provides a basis for further dialogue and work on the reform initiatives and their effective management. Major findings include:

- While reforms have taken off in some segments of the economy, public and foreign confidence in the investment climate continue to be eroded by a lack of clarity on policy and the legal environment, as well as uncertainties regarding the enforcement of the rule of law.
- Better alignment of resources and expenditure obligations and greater accountability of public institutions are necessary to ensure that resources are properly harnessed to construct the physical infrastructure needed for economic growth. Finally, an efficient civil service—driven by the right incentives framework, a strong sense of professionalism, and high ethical standards—is indispensable to the implementation of Indonesia's economic and social agenda.
- Evidence shows that weak corporate governance practices in most of Indonesian companies have led to many deficiencies in their decision making and corporate actions: inefficient investments, high financial leverage, maturity mismatch of borrowings, and unhedged foreign exchange exposures.

Assessment of shareholders' role and major constraints. Policy implications of these findings on the limitation of the effectiveness of shareholders' rights could be to encourage more active dissemination of corporate governance information beyond the legal minimum. This approach of effective dissemination of information may not always appear to be in the direct interest of the majority shareholder, but once directed it is expected to improve the monitoring of the firm's performance and therefore its value to all shareholders. Current regulations on shareholders' rights are adequate, but the attitude of companies toward their shareholders (and vice versa) as stakeholders, and not only as providers of capital, needs to be changed if corporate governance is to improve. A survey finding indicated that only few corporate respondents have their own web sites. Companies should also update their web sites with the latest condition of their companies, including their corporate governance condition. A comprehensive corporate web site is very valuable for shareholders in order to protect their investment.

Lessons learned. Effectiveness of the board of directors and board of commissioners regulatory reform and related developments geared to enhancing the effectiveness of the boards.

Minimum number of independent commissioners. Both Company Law and Capital Market Law do not recognize "independent commissioner" and/or "independent director." The terminology of "independent commissioner" was introduced by the JSX regulation in the year 2000 (and the later revised regulation in 2001). The JSX regulation requires publicly listed companies to appoint independent commissioner(s). Listed companies are obliged to have independent commissioners proportionally equal to the shares owned by the noncontrolling shareholders. There is no additional and particular role of independent commissioners in the JSX regulation other than the role as set out in Company Law (i.e., to supervise and give advice to the board of directors). However, the National Code for Good Corporate Governance emphasizes the role of all board of commissioners members to ensure that the company performs its social responsibilities and considers the interests of various stakeholders of the company as well as monitoring the effectiveness of the Good Corporate Governance practices.

Board committees. Both Company Law and Capital Market Law do not stipulate committees, which may be established by the board of commissioners. The Bapepam (government regulatory agency) chairman issued a circular letter in 2000 that recommends publicly listed companies establish audit committees. This recommendation is attributed to the publicly listed companies and public companies in order to heighten accountability as carried out by the board of commissioners.

Minimum number of board meetings. Both Company Law and Capital Market Law do not provide any clear requirement for the board of commissioners (BoC) and the board of directors (BoD) to hold a meeting. However, since the BoC has to sign the annual report of the company together with the BoD, it is

intended that the BoC may also hold a meeting to discuss such a matter. With the Code provisions regarding the requirement of the BoD to make and maintain the minutes of the BoD meeting and to prepare the business plan and annual report of the company, it is intended that the BoC may also hold a meeting to discuss such a matter. However, according to the Code there is stipulation that the BoC meetings should be held regularly, at least once every month in principle, depending on the specific characteristics of the company. The BoC should adopt procedures for its meetings and should clearly set out such procedures in the minutes of its meetings, noting when such procedures were determined and decided.

Commissioners and directors. The following conclusions were made:

- Education and training for directors and commissioners, beyond what is mandatory, are still rather uncommon; 53 percent only occasionally give such training, and the remaining 47 percent never. None of the companies actively provides training.
- A minority of the companies provide a contact person for the support of independent commissioners.
- Few companies (6 percent of the respondents) have effective formal mechanisms for the evaluation of the performance of directors.
- The independent commissioners do not often meet with managers or employees of the companies in order to obtain direct information about the company's state of affairs. Some 65 percent of the respondents indicate that the independent commissioners meet "sometimes," and 24 percent indicate that they meet "rarely" with managers and employees.
- The majority of the companies (73 percent) indicate that the independent commissioners have unrestricted access to the company's documents and accounting system. Many respondents (45 percent) acknowledge that the independent commissioners do not always receive adequate information in time to process before every meeting of the commissioners.
- Only one-third of the respondents indicate that their company allows them to seek outside legal, financial, and other expertise at the company's expense. More than half of the companies allow it only in exceptional cases. There are therefore noticeable limitations on the freedom of additional support for commissioners to carry out their tasks.
- Almost all directors and commissioners surveyed regard the payment for independent commissioners to be adequate or better. There is, however, also a general major concern over the liabilities of the commissioners.
- The overall corporate governance score of companies in Indonesia showed very little variation over the different forms of ownership and control. Diffusely owned firms and firms with professional managers not related to the controlling shareholders showed only a marginally better corporate governance than other companies.

(B) Assessment of the Effectiveness of the Boards and Future Tasks

In assessing the effectiveness of the boards, the following conclusions can be drawn from the recent legal developments and the survey findings:

- *Appointment of the independent commissioners.* There have been some improvements in the effectiveness of the boards in recent years. Some listed state-owned enterprises (SOEs) for the first time in their long histories have decided to appoint independent commissioners through a relatively fair and transparent process. These independent commissioners (including those of non-SOE listed companies) are expected to initiate and promulgate the implementation of Good Corporate Governance in their companies. By having the independent commissioners in the BoC, it is hoped that the BoC will be able to have a more independent voice and position toward the BoD. Survey findings indicate that almost all listed companies have independent commissioners who, according to JSX data, meet the criteria of independence.
- *Establishment of audit committees.* In accordance with the regulations, 84 percent of the listed companies now have an audit committee. This committee of the BoC should be led by an independent commissioner, which is the case in 100 percent of audit committees in the companies surveyed. The committee's main function and role in Indonesia's listed companies (regulated by JSX circulars and Bapepam, or SOE ministerial decrees for SOEs) are focused on three aspects:
  1. Improving the company's financial reporting
  2. Overseeing the implementation of Good Corporate Governance (GCG)
  3. Corporate control

  In context, it is too early to say that audit committees have been effective in carrying out their duties and because of that have improved the effectiveness of the boards, but the establishment of the audit committee is a very important milestone to that improvement. The survey findings indicate that good progress has been made in establishing audit committees in a relatively short time. Their focus so far appears to be on internal auditing, more than on external auditing.
- *Board of commissioners meetings performance.* Besides the appointment of independent commissioners and the establishment of the audit committee, the improvement of effectiveness of the boards can also be seen through their presence in the commissioners meetings. Because these meetings should be reported in the Annual Report as well as their performance in attending the meetings, the presence of the members of the BoC in commissioners meetings has improved. The survey findings indicate that almost all listed companies have independent commissioners who do actively participate in the board meetings and their opinions are recorded. However, the independent commissioners do not often alter the agenda as set by the president-director or disapprove agenda items.

- *Shareholders' role in corporate governance.* Policy implications of these findings of the limitation of the effectiveness of shareholders' rights could be to encourage more active dissemination of corporate governance information beyond the legal minimum. Current regulations on shareholders' rights are adequate; however, some modifications of the General Meeting of Shareholders (GMoS) provisions should be taken into consideration, such as to make it compulsory for a company to hold an extraordinary GMoS in case of a bad financial situation. Additionally, more could be done to inform shareholders about their rights. This could be a task for the JSX. If corporate governance is to improve, the attitude of companies toward their shareholders (and vice versa) needs to change to recognize shareholders as being stakeholders and not only providers of capital. Overall, findings indicate that the meetings of the board of commissioners are generally forums for serious discussion but that the BoC does not really have much influence on the company's management and policy. Companies have not yet provided a lot of supporting facilities, such as education and training, to enable to commissioners to carry out their duties.
- *Recommended future tasks.* The role of the BoC needs to be strengthened and its effective influence on the management and policy of the company needs to be brought in line with its responsibilities. One of the future tasks of the BoC is to implement a fair and transparent performance measurement and remuneration system for the BoD, which has mostly not yet been carried out.

Another most important task is to clearly define the meaning of the independence of the independent commissioner and its legal status, because the JSX regulation does not give any indication for the placement of independent commissioners in the BoC. The Company Law stipulates that the BoC is by nature an independent body, and thus the so-called independent commissioner would seem to be unnecessary. But in practice, the independence of the BoC is hardly achieved, and thus it needs the implanting of an outside/independent commissioner(s) to forcibly improve its independence.

Companies should also consider bringing their BoC in line with the ideal size of BoC composition. ADBI suggested that the ideal BoC consists of 10 commissioners. Education or training for commissioners to improve their capabilities and knowledge, especially their responsibilities and liabilities under the law, should be also encouraged.

50.4 CONCLUSION

Indonesia needs to promote and implement findings and recommendations of studies and reports conducted on the nation's performance regarding corporate governance from a broad range of institutions.

The government should commit itself to establishing a committee of public and private sector officials to recommend actions and policies to be implemented

to strengthen legislation guiding corporate companies. Sufficient resources will be required to provide oversight and enforcement of regulations. Companies must implement and institute transparency and openness within and outside the organization with strict reporting requirements necessary if full confidence is to meet public expectations.

A need exists for proper education of all sectors of society as to the importance of corporate governance, and rules and regulations guiding government policies should be adequately funded and supported. To gain the international confidence of the global economy, Indonesia needs to become a world trade partner by becoming a leader in meeting the goals of good corporate governance. For, as the OECD noted, "Good corporate governance underpins market confidence, integrity, and efficiency and hence promotes economic growth and financial stability."[17]

50.5 REGULATIONS

1. Indonesia, Law Concerning Limited Liability Company, Law No. 1, year 1995.
2. Indonesia, Law Concerning Capital Market, Law No. 5, year 1995.
3. Indonesia, Law Concerning Prohibition of Monopolistic Practices and Unfair Competition, Law No. 5, year 1999.

Notes

1. *CIA Fact Book*, December 2006. https://www.cia.gov/cia/publications/factbook/geos/id.html.
2. Asia Corporate Governance Association, Country Snapshots 18-Dec-2004. "The Economic Crisis in East Asia: Causes, Effects, Lessons," by Martin Khor, director, Third World Network, 1998. www.ifg.org/khor.html.
3. www.acga-asia.org/public/files/IndonesianCode_2001.pdf.
4. Ibid.
5. "Corporate Governance Disclosures in Indonesia: A Study of LQ45 Companies," www.cgfrc.nus.edu.sg/publications/cg_dis_indon.html.
6. www.clsa.com.
7. www.acga-asia.org/content.cfm?SITE_CONTENT_TYPE_ID=11&COUNTRY_ID=265.
8. ACGA's third annual conference in late 2003.
9. "CLSA Asia-Pacific Markets/Asian Corporate Governance Association," www.acga-asia.org/content.cfm?SITE_CONTENT_TYPE_ID=19.
10. "CLSA Asia-Pacific Markets/Asian Corporate Governance Association."
11. Asian Corporate Governance Association (ACGA), "A Preview of CG Watch 2005," presentation by Jamie Allen, Secretary General, at the OECD 2005 Asian Corporate Governance Roundtable, September 8, 2005, Bali.
12. "CG Watch," a joint report by CLSA Asia-Pacific Markets and ACGA.
13. www.cic-fcgi.org/news/files/BUKU1-english.pdf.

14. www.worldbank.org/ifa/rosc_cg_idn.pdf.
15. Jakarta Stock Exchange and PricewaterhouseCoopers, Corporate Governance 2002 Report on Institutional Investor Survey, Jakarta, September 2002.
16. www.adb.org/Documents/Reports/CGA/ino.asp.
17. "The Revised OECD Principles of Corporate Governance: A Management Roadmap for Healthy, Well-Governed Companies," remarks by Bill Witherell, Director for Financial and Enterprise Affairs, OECD, at the CFO Strategies: Corporate Accountability Forum 2004, Monaco, May 17, 2004.

References

Asian Development Bank (ADB). 1999. *Corporate governance and finance in East Asia: A study of Indonesia, Republic of Korea, Malaysia, Philippines, and Thailand*. Vols. 1 and 2. Ed. Ma Virginita Capulong, David Edwards, David Webb, and Juzhong Zhuang.

Bapepam. 2002 and 2003. Annual press release.

Black, Henry Campbell. 1996. *Black's law dictionary: Definition of the terms and phrases of American and English jurisprudence, ancient and modern*. St. Paul, MN: West Publishing Co.

Clark, Robert C. 1986. *Corporate law*. Canada: Little, Brown & Company Limited.

Jakarta Stock Exchange and PricewaterhouseCoopers. 2002. Corporate governance 2002 report on institutional investor survey. Jakarta, September.

Kaufmann et al. 2006.

Musa, Soebowo, and I Putu Ary Suta. 1999. Membedah Krisis Perbankan: Anatomi Krisis dan Penyehatan Perbankan, Yayasan Sad Satria Bakti, Jakarta, Indonesia.

Pangestu, Mari, and Farid Harianto. Corporate governance in Indonesia: Prognosis and way ahead. Presented at the International Conference on Democracy, Market Economy and Development, Seoul, South Korea, February.

Peij, S. C., et al. 2002. *Handboek corporate governance*. Deventer, Netherlands: Kluwer bv.

Simandjuntak, Djisman S. n.d. Good corporate governance in post-crisis Indonesia: Initial conditions, windows of opportunity and reform agenda. Taken from www.unescap.org/drpad/publication/fin_2148/chap2.pdf.

Santoso, Wimboh. 2002. Indonesia's financial and corporate sector reform. Banking Research and Regulation Directorate, Bank Indonesia, Jakarta.

CHAPTER 51

COMPLIANCE: BRAZIL

L. Nelson Carvalho, PhD
Elionor Weffort, PhD
Bruno Salotti, PhD

51.1 INTRODUCTION

In both area and population, Brazil is one of the largest countries in the world, and it is classified as a developing economy. Due to the vast latitude of this poorly defined expression, it is worth pointing out certain features of the country's current economic status to properly frame the understanding of its present compliance regime.

An old-time exporter of commodities (only gold and coffee made the country famous in the then developed European courts between the sixteenth and nineteenth centuries), Brazil nowadays hosts a very diversified and modern industrial base and a world-class services industry.

About 70 percent of its exports are composed of either services or manufactured and semimanufactured products; the efficiency of its steel mills and mining exploration ventures (privatized in the early 1990s) is recognized worldwide, which also makes them global players and key foreign investors. Manufacturing and exports of passenger aircraft propelled Brazil's high-technology industry to the level of competition with soundly developed economies. The Brazilian

banking system is highly sophisticated and extremely efficient both at home and abroad, and its largest private banks are currently acquiring financial institutions in the neighboring Latin American countries, in a clear move to get prepared to invest in the banking industry of developed economies; besides, Brazilian banks are permanent acquisition targets for world giant financial institutions.

After its privatization back in 1998, the telecom industry—substantially driven by foreign investment—was able to increase its reach to the population, due to the high technological level of its services and the cost reduction to consumers, to well over one hundred million units in operation of mobile and fixed line phones in 2006. Nevertheless, its agro-industry was able to achieve increasing degrees of effectiveness and its agricultural output growth launched Brazil to the first position as a well-respected and important exporter; its biofuel chemical research in the 1970s managed to permit adoption of sugarcane-based ethanol as an answer to the several-fold increase in the cost of imported oil, and its flex-fuel fleet is today one of the largest in the world. (Brazilian technology for ethanol combustion engines is famous among developed and developing economies alike.) In spite of that, continuous and successful search of new fields, inland and offshore, by its giant oil company Petrobras led to the announcement in 2006 that Brazil will be totally self-sufficient in oil production before the end of the decade of 2000–2010. Its iron ore mining giant company Companhia Vale do Rio Doce completed in late 2006 the acquisition of a large mining concern in Canada and became a US$70 billion plus stock market capitalization worth listed company in the largest stock exchanges in the northern hemisphere on both sides of the Atlantic and in the Asian markets.

All this surge in development was highly motivated by the extremely well-conceived and better-implemented stabilization plan of the economy launched by the government in 1993, and that was able to tame the 40-year plus long two-digit annual inflation rate for the past almost 15 years since then; inflation in 2006 was around 4 percent.

On the dark side, decades of federal budget deficits financed by expanding inflation could result in no little pain to balance the federal budget. The price still being paid is a huge government incapacity to reduce taxes to a fair level, imposing a burden that impairs enterprises to invest increasingly more in the short and medium terms. Inheritance of a labor legislation that was modern when it was implemented in the 1940s but saw little improvement since then adds an additional and relevant bill to the cost of managing the workforce—costs of keeping people in the payroll and, worse, of firing idle personnel tend to disincentive hiring. Social security displays enormous deficits that must be covered by an ailing cash flow at the Treasury Department, forcing interest rates to skyrocket to help balance the federal budget by issuing public debt attractive to investors. This equation will require reforms in labor, tax, and social security legislation that may call for a mature consensus among the political clans and by society, which does not seem close to be achieved.

Even in the light of the reforms needed and that don't show signs of prospering in the short run, the country experimented a cycle of expansion of its business environment, and was able to virtually get rid of its formerly costly and short-term-due foreign debt with the help of the high liquidity of the world economy in the past few years. Foreign credit and foreign direct investment poured in at a high pace in the past ten or so years, and no few economists believe that the country may target to achieve an "investment grade" status by 2012 if the public fiscal discipline that was implemented from 1994 to 2006 continues, as there is explicit evidence that it will.

This entire scenario brings about a reflection on how the legal system is set to accommodate the settlement and development of businesses that may come from the positive growth perspectives in economic activity, and how standards-setting and infralegal regulation or self-regulation may contribute to an environment of compliance with benchmark practices that by themselves stimulate investments.

51.2 BUSINESS OWNERSHIP STRUCTURE AND PUBLIC ACCOUNTABILITY

The state still plays an important role as entrepreneur, no longer in number of companies it owns but in relation to their size. In spite of a wide and deep privatization program of state-owned companies in the 1990s, a few very large companies are still government-owned: the oil company Petrobras, virtually all of the hydroelectric generating companies, and the country's largest bank (Banco do Brasil), to name the main ones.

Businesses may take the form of limited liability companies or, alternatively, of corporations—these may be listed or not. Around 40 of the largest companies listed in Brazil also trade securities in foreign stock exchanges, either under regular listing or via American depositary receipts (ADRs) in New York, Latibex in Spain, and other markets.

Company law requires all companies to prepare annual financial statements (semiannual statements are required by the regulators for financial institutions and insurance companies). Only private listed companies and all government-owned enterprises—listed or not—and all banks and insurance companies are required to hire independent auditors. Limited liability companies are exempted from any requirement to disclose their financial position and results of operations in any form other than filing tax returns. This apparently bureaucratic and harmless piece of legislation hides a potential threat to corporate governance and general disclosure of business activities in Brazil: Under the protection of such exemption, many (virtually all) Brazilian subsidiaries of very large U.S., Japanese, and European corporations listed in their home countries opt for the form of limited liability companies in Brazil, and do not feel accountable to report their financial performance at any forum in their host Brazil.

51.3 LEGAL ENVIRONMENT

The efforts to move a formerly colonial-minded commodity exporting economy that prevailed to the end of the nineteenth century into an industrialized one led the governments from 1930 on to set up companies and to become entrepreneurs. State-owned companies popped up and played a key role to permit partnership with private investors and led to a nontrivial capacity of occupying space for substitution of imports and job creation. This proved effective for most of the past century, and at its end it became clear that the conditions were in place to privatize most state-owned companies and abandon the model of such a heavy state intervention in the production mechanisms.

This radical change in enterprise ownership oriented a great deal of the legislation about doing business in Brazil in the last half of the twentieth century.

The Brazilian legal system is predominantly Roman-German, or statutory. However, specifically regarding business law, a strong influence of common law can be verified.

The Federal Constitution (1998 and further amendments) holds the general principles of financial/economic activities, such as private ownership, free competition, consumer protection, and environment protection, and also handles the issue of regulated industries. The main pieces of legislation ruling business activities are found at the infra-constitutional level, such as the Civil Code (2002), the Company Law (1976 and further amendments), and the Bankruptcy Law (revised in 2005).

In addition to the Constitution and the aforementioned legislation, the following regulatory agencies are authorized to set standards and rules of conduct for business enterprises: Central Bank of Brazil (financial institutions); Brazilian Securities and Exchange Commission (CVM) (listed companies); Superintendency for Pension Funds (SPC); and Superintendency for Insurance Companies (SUSEP). An attempt to implement the concept of regulatory agencies for other regulated industries like power generation, water treatment and supply, and civil aviation, for instance, is still in its infant stage and cannot be referred to as a successful experience. The implementation of the older regulatory agencies in Brazil, with a mandate for regulation and supervision, depicts the influence of common law.

Exhibit 51.1 is a sample list of sectors that need to comply with regulatory requirements and the main entities (with their related Internet sites) responsible for regulation and control of these sectors.

The pyramid in Exhibit 51.2 synthesizes, hierarchically, the main sources of influence over the denominated business law in Brazil. In the event of any lack of rules, general principles of law are to be applied by analogy.

This section mainly deals with the listed companies' environment, for analysis of compliance, as they are the major targets of regulations in this respect, in spite of representing no more than 700 companies in the universe of 20,000

Sector of Economy	Entities Responsible for Regulation and Control	Site (Site Language)
Financial institutions	Brazilian Central Bank	www.bcb.gov.br/?english (English)
Insurance, capitalization, and pension companies	Superintendence of Private Insurance and Complementary Pension Secretariat	www.susep.gov.br/menuingles/about bim.asp (English) www.mpas.gov.br/spc/legis/ index.asp (Portuguese)
Electricity companies	Electricity Regulatory National Agency	www.aneel.gov.br/default.cfm? idioma=1 (English)
Telecommunication companies	Telecommunications Regulatory National Agency	www.anatel.gov.br/home/default/asp (Portuguese)

EXHIBIT 51.1 SAMPLE LIST OF BRAZILIAN SECTORS

plus corporations in Brazil. The nonlisted ones and the limited liability companies, well above that number, fall short from a minimum level of compliance requirements other than for their tax obligations.

Corporation shares may be common or preferred. The law permits rights that may be assigned to founders, known as fruition shares, but these are not usually found in practice. Common and preferred shares represent the corporate

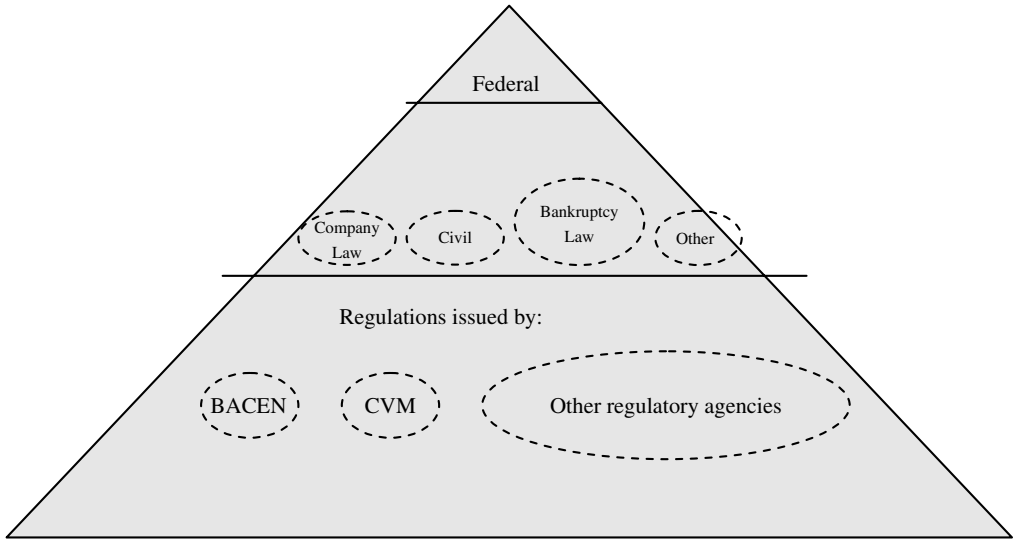


EXHIBIT 51.2 HIERARCHICAL PYRAMID

capital, while fruition shares are only securities, with rights specified in the bylaws and/or deliberations of shareholders' meetings, granted to former holders of shares, which were amortized by the company by means of payment of the face value to their holders.

A common share is different from a preferred share in relation to the rights of their holders: While the former—of mandatory issuance—grants its holders the right to vote and receive dividends, the latter provides preferences or advantages, such as priority in the distribution of dividends and capital refund, and entitle their owners to tagging along at least 80 percent of the price paid by the acquirer in the case of change in control of the voting stock. Preferred shares give no voting rights or in certain cases permit voting in a limited number of cases they specify.

With amendments voted in 2001 to the 1976 Company Law, the total number of preferred shares may not exceed the total amount of shares of the company by 50 percent. Prior to this change in law, up to two-thirds of preferred shares could be issued.

Listed companies are also entitled to issue share subscription bonuses as well as other securities in the form of debt, like debentures, commercial papers, and depositary receipts.

The setting up of a listed corporation depends on a financial institution (underwriter) that will subscribe and/or place the shares in the market.

Next, the phases for setting up a corporation in Brazil are briefly described:

1. Request for issuance registration with the Securities and Exchange Commission, containing, as a minimum: a study of economic and financial feasibility of the business, project of bylaws and a prospect with the amount of capital to be subscribed, number, kind, and class of shares
2. Minimum subscription of 50 percent (banks) or 10 percent (other companies) of shares through public placing of shares intermediated by the underwriter
3. Designation by the founders of a formation or organization meeting for approval by the majority of the partners
4. Filing of the bylaws and other documentation required by law with the local Registry of Commerce or its head office

Upon the fulfillment of these phases, the company may begin its activities, subject to the continuous supervision from the Brazilian Securities and Exchange Commission (CVM) and such other regulating agencies, if applicable to its line of business.

Three bodies are fundamental for the operation of all publicly held companies: shareholders' meetings, board of nonexecutive directors, and a board of statutory executive directors or officers.

A statutory audit committee is mandatory for companies where there is governmental shareholding and for other companies when their bylaws so determine.

The shareholders' meeting is the most important deliberation body of a company, gathering all shareholders with or without voting rights. There are no restrictions as to the matters to be deliberated in the shareholders' meetings; however, depending on the subject, a specific quorum may be required.

The board of directors and the statutory executive officers share the supervision and management of the listed company, respectively. The board of directors—formed by at least three individual shareholders or by parties appointed by them—is empowered to set the general business orientation of the company; convene shareholders' meetings whenever they deem necessary; and elect, dismiss, and inspect officers pursuant to the Corporations Law. The executive officers—at least two members, shareholders or not—are empowered to execute deliberations of the shareholders' meetings and the board of directors and run the company.

The statutory audit committee is empowered mainly to monitor the compliance of financial statements with the Company Law, as well as monitor the administrators' acts and investigate any charges of errors or frauds. It was conceived in a 1940 version of the Company Law as some sort of an audit committee with functions not so ample as today's committees, and it has been temporarily accepted by the U.S. SEC as a substitute for audit committees for Brazilian companies trading securities in the United States.

The Brazilian civil code defines general rules that Brazilian companies must comply with, such as bookkeeping criteria and accountant responsibilities for properly maintaining the companies' books.

51.4 ACCOUNTING/FINANCE ENVIRONMENT

The requirements of the accounting environment are essentially influenced by the company's legal structure. The corporations, listed or not, are regulated by the Company Law, which embodies both *general* rules (such as which are the obligatory financial statements and the frequency with which they have to be published), as well as *specific* rules (like how items shall be displaced in the body of the mandatory financial statements as well as some basic accounting standards like the use of the lower of cost or market measurement for selected asset items).

The basic financial statements a company must publish in at least one Brazilian newspaper annually are the balance sheet, the income statement, a statement of changes in shareholders' equity, and a statement of source and application of funds. The third one may be substituted by a statement of changes in accumulated profit and loss (a limited version of statement of changes in shareholders' equity), and the last one may not be published by private companies that have shareholders' equity inferior to one thousand reals (about US$500 at December 31, 2006). Companies must follow Brazilian generally accepted accounting principles.

According to CVM (Brazilian SEC) rules, the statement of changes in shareholders' equity and the statement of source and application of funds are

obligatory. Besides, interim financial statements must be presented to the Commission quarterly and also must comply with the Commission's rules.

Companies from specific sectors may face the need to comply with additional requirements coming from their regulatory agencies; for example, electricity companies must elaborate and publish two supplementary financial statements: the cash flow statement and a value-added statement.

A great step forward in the harmonization of Brazilian accounting standards with international ones was given in March 2006, whereby the Brazilian Central Bank started a formal convergence project toward the adoption of the International Financial Reporting Standards (IFRS) issued by the International Accounting Standards Board (IASB) as of the year ending December 31, 2010. This decision to converge high-level international standards represents a significant evolution in the quality and transparency of financial statements of financial institutions in Brazil. Additionally, for over ten years now, accounting rulings issued by the CVM aiming at listed companies have already been closely following the orientation in the standards set out by the IASB, and it is expected that shortly CVM and other regulatory agencies will take formal steps of convergence toward IFRS just like the Central Bank did in 2006.

The accounting profession is regulated by the CFC—the Federal Accounting Council and its related system of state (regional) accounting councils (CRCs). Accountants must be registered at a CRC after graduation in order to be authorized to practice. Although the mission of the Federal Accounting Council is to monitor the professional practice of accountants, in order to do so it felt it should develop accounting standards and rules that must be complied with by any accountant registered at any regional accounting council.

Accounting standards also come from pronouncements issued by the Institute of Independent Auditors of Brazil (Ibracon), which have no enforcement power but usually are officially adopted by the CVM, which then makes them enforceable.

All Brazilian companies that have their shares publicly traded must get listed at the São Paulo Stock Exchange (Bovespa), which has self-regulatory powers. Thus, Bovespa may suspend the trading of securities issued by the companies or may cancel their trading license.

In 2000, Bovespa created an elite level of listing called "New Market" (Novo Mercado). According to its web site,[1] "The Novo Mercado is a trading segment designed for shares issued by companies that voluntarily undertake to abide by corporate governance practices and transparency requirements in additional to those already requested by the Brazilian Law."

Since its creation, the number of companies adhering to the New Market continues to grow. According to a September 2006 Bovespa Bulletin,[2] there are 83 companies that are listed on this market, representing more than 20 percent of the number of total listed companies listed at Bovespa but accounting for a much higher percentage of the total market capitalization.

There are three levels of this new market. These levels represent a scale related to the adoption of corporate governance principles. The most demanding level requires that the company must have its capital divided only by common (fully voting) shares, therefore forbidding any form of preferred shares. Details of all requirements may be accessed at the Bovespa web site (www.bovespa.com.br).

Companies that have shares traded in other markets, such as the NYSE (usually in the form of American depositary receipts), must comply with specific regulation from these markets.

Banks with stockholders' equity above certain minimums are required to have audit committees, and in certain cases the audit committees must have a majority of outside members and necessarily an accounting and finance expert. Audit committees reports are filed with the Central Bank semiannually, and summaries must be published with the financial statements. Central Bank rulings relating to compliance are extremely detailed, and a statutory executive director holds legal responsibility for overseeing each bank's compliance function.

51.5 AUDITING ENVIRONMENT

The auditors play an important role toward the achievement of proper levels of compliance, as a consequence of their responsibility to go through the companies' internal control and compliance procedures aiming at rendering opinions on the financial statements of their clients. It is worth remembering that only listed companies, banks, insurance companies, and government-owned ones are required to have financial statements audited by independent auditors. Limited liability companies, by far in larger number than corporations and encompassing very large privately owned domestic and foreign enterprises, are exempted by law from any kind of public accountability.

Auditing is not a separate profession in Brazil; the audit function is formally an extension of the practice of accounting, and auditors are considered specialized accountants and therefore fall within the supervisory capacity of the Federal Accounting Council. Auditing requirements are also issued by the Central Bank, the Superintendency of Insurance Companies, and the Securities Commission. All major international accounting firms have offices in all major Brazilian cities, some since almost 100 years ago. Audit firms must be registered at the Securities Commission and are peer reviewed on a periodic basis. Besides, the Federal Council of Accounting set out a Continuous Education Program requiring a number of education credits to be met by auditors every year.

51.6 CORPORATE GOVERNANCE IN BRAZIL

No more than ten years ago, sound corporate governance practices were largely ignored in Brazil. The extensive use of the legal right to issue up to two-thirds of preferred (nonvoting) shares gave listed companies room to have controlling shareholders actually unaccountable for their acts due to their ability to decide the course of action of the companies even owning no more than 17 percent of

the company's total stock, equivalent to 50 percent plus one share of the voting stock.

Globalization of financial markets was key to completely change that scenario: Brazilian companies that got listed in foreign developed stock markets partnered with foreign investors eager to participate as their shareholders in the Brazilian stock market.

Such partnership developed wonders to upgrade and enhance sound corporate governance practices domestically. CVM and the São Paulo Stock Exchange (Bovespa) each set out their own guides of sound corporate governance practices to be mandatorily complied with.

A not-for-profit organization known as the Brazilian Institute of Corporate Governance (IBGC) reshaped itself from the old form of the Brazilian Institute of Board Members and is extremely active in producing papers and books, and in organizing domestic and international seminars and conferences on corporate governance. It has several courses on the subject, including mock meetings of boards with auditors and with management, besides having published a comprehensive booklet on benchmark corporate governance practices, another on audit committees, and a third one on statutory audits and statutory auditors. IBGC is a member of a number of similar international organizations, like the International Corporate Governance Network (ICGN), and IBGC members are leaders of World Bank initiatives to disseminate good corporate governance practices, mainly in Latin America.

51.7 SHORTFALLS IN THE LEGAL ENVIRONMENT

Two issues are considered relevant to be overcome in order to fasten the achievement of benchmark levels of compliance requirements in Brazil.

The first one has to do with the judicial system, which is absurdly slow to decide cases and which is construed in such a way that a formidable set of procedures are accepted by courts that have as a final result a level of procrastination to hear cases and to come to final solutions that prevent justice to be made within a reasonable period of time for the injured parties. This legal framework is so worrying that the Bovespa New Market initiative requires companies to change their bylaws to formally commit themselves to sending disputes with shareholders to arbitration and not to the courts, in an attempt to shorten the time frame between opening and settling the dispute.

The second issue relates to the exaggerated interference of the Internal Revenue Service requirements in the field of financial accounting. Due to the long-established culture from the beginning of the past century, when capital markets simply existed in Latin America and in Brazil in particular, tax accounting requirements started to be imposed on companies that filed tax returns—which may be considered normal—but were aggravated by the requirement to have those tax accounting treatments booked in the financial accounting records and reflected in the resulting financial statements. Matters such as limits to deductible

depreciation, deductible allowance for bad debts, amortization of intangibles, and certain liability accruals, for instance, were reflected in the financial statements designed to guide investors' economic decisions regardless of the underlying economics.

Although this situation is better today than it was before the regulatory bodies started to deal with the distortions in financial information stemming from that practice, it will only be resolved when an 11-year-old project of law is voted and sanctioned that will ultimately segregate tax from financial accounting.

51.8 COMPLIANCE AND ITS DEPENDENCE ON THE FUTURE OF ACCOUNTING STANDARD SETTING IN BRAZIL

As mentioned, Brazil is making efforts to converge with international financial reporting standards, and the sooner it approves the project of law freeing financial accounting from undue income tax accounting restrictions, the earlier convergence will be achieved.

Meanwhile, six entities started an initiative a couple of years ago, and in the second half of 2006 finally an accounting standards setting organization was founded. It is the Committee on Accounting Pronouncements (CPC), formed by founding members Bovespa (the São Paulo Stock Exchange); the Foundation Institute for Research on Accounting, Finance, and Actuarial Sciences (FIPECAFI), representing the academic world; Ibracon (the Institute of Independent Auditors of Brazil); the Federal Council of Accounting (CFC); and the Association of Investment Professionals in the Capital Markets (APIMEC), or the analysts; and the Association of Brazilian Listed Companies (ABRASCA).

This recently founded body, CPC, is already working in converging Brazilian accounting standards toward the ones coming from the IASB, and it is hoped that CPC will see its powers enlarged when the project of law mentioned in the preceding section passes through Congress and is transformed in law, to the extent that the current restrictions preventing the adoption of best accounting practices in financial reporting will then have gone.

Notes

1. www.bovespa.com.br/Companies/NovoMercadoSpecial/NovoMercadoi.htm.
2. www.bovespa.com.br/pdf/BoletimInformativo92.pdf.

CHAPTER 52

CANADIAN SOX (BILL 198)

Madeleine Ferris Shaw
Sanjay Anand

52.1 BACKGROUND

In 2002, the Ontario Securities Commission (OSC) introduced Bill 198 in response to the reforms taking place in the United States under the Sarbanes-Oxley Act (SOX) and to regain the confidence of investors in Canada's capital markets. Just as the United States saw a number of fiascoes and accounting scandals like Enron and WorldCom, so did Canada with companies like Parmalat and Nortel. Not surprisingly, therefore, Bill 198 is often referred to as Canadian SOX (CSOX).

The purpose of Multilateral Instrument 52-109 (MI 52-109) Certification of Disclosure in Issuers' Annual and Interim Filings is to improve the quality and reliability of reporting issuers' annual and interim disclosures. The initial phase of the ruling required CEOs and CFOs certify that:[1]

- They have designed, or supervised the design of, internal controls and implemented those controls to provide reasonable assurance that the issuer's financial statements are fairly presented in accordance with generally accepted accounting principles.
- They have designed, or supervised the design of, disclosure controls and procedures and implemented those controls to provide reasonable assurances that material information relating to the issuer, including its consolidated subsidiaries, is made known to them by others within those entities.

- Annually, they have evaluated the effectiveness of their internal controls and disclosure controls and procedures and presented their conclusions regarding the effectiveness of those controls in the annual Management, Discussion, and Analysis (MD&A).
- They must disclose to the issuer's audit committee and independent auditors any significant control deficiencies, material weaknesses, and acts of fraud that involve management or other employees who have a significant role in internal controls. Any significant changes to the controls must be publicly disclosed in the issuer's annual and interim MD&S.

The degree of complexity or specific policies or procedures that must make up an issuer's internal controls or disclosure controls are not prescribed. The approach to be taken is left to the judgment of the issuer's CEO and CFO based on reasonable controls that take into account the issuer's size, the nature of its business, and the complexity of its operations.

There are also two other policies issued by the OSC that were developed to enhance investor confidence and to maintain the reputation that of the Canadian capital markets internationally. The purpose of Multilateral Instrument 52-108 (MI52-108)—Auditor Oversight is "to contribute to public confidence in the integrity of financial reporting issuers by promoting high quality, independent auditing."[2] It requires that the reporting issuers:

- Engage auditors that participate in an independent oversight program established by the Canadian Public Accounting Board (CPAB) for public accounting firms that audit the financial statements of public companies (the CPAB Oversight Program)
- Are participants in good standing with CPAB

The purpose of Multilateral Instrument 52-110 (MI52-110)—Audit Committees is "to encourage reporting issuers to establish and maintain strong, effective and independent audit committees." The Audit Committee Rule is derived from the audit requirements administered by the U.S. Securities and Exchange Commission (SEC) as well as the listing requirements of the New York Stock Exchange (NYSE) and NASDAQ Stock Market. MI52-110 defines the meaning of independence and the educational and/or experience requirements of a member of the issuer's audit committee. Some of the responsibilities of the audit committee include:

- Overseeing the work of the external auditors including audit and nonaudit services
- Reviewing the issuer's financial statements, MD&A, and earnings press releases before the issuer publicly discloses this information
- Ensuring that adequate procedures are in place for the review of the issuer's disclosure of financial information extracted or derived from the issuer's financial statements

- Establishing procedures for:
  - The receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters
  - The confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters

The audit committee also has the authority:

- To engage counsel and other advisors as it determines necessary to carry out its duties
- To set and pay the compensation for any advisors employed by the audit committee
- To communicate directly with the internal and external auditors

Initially, the OSC proposed compliance with Multilateral Instrument 52-109 (MI 52-109) Certification of Disclosure in Issuers' Annual and Interim Filings and Multilateral Instrument 52-111 (MI 52-111) Reporting on Internal Control over Financial Reporting. The requirements of these were substantially similar to those of SOX 302 and 404 Rules. The intent was a phased approach including the CEO/CFO review of the filings ("bare" certificate); the design of disclosure controls and procedures including the recording, processing, and summarization of filings, and assessment of the effectiveness of these control and procedures ("modified" certificate); and the design and testing of the internal control system ("full" certificate). After considering the feedback received during the comment period from a wide range of stakeholders and recent developments internationally, particularly in the United States, the OSC expanded MI 52-109 to include the internal control reporting requirements. (See Exhibit 52.1.)

The most significant difference is that the issuer will *not* be required to obtain from its external auditor an internal control audit opinion concerning management's assessment of the effectiveness of internal control over financial

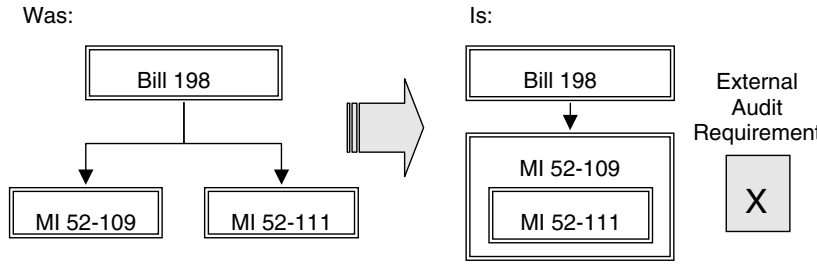


EXHIBIT 52.1 EVOLUTION OF BILL 198

reporting. The removal of the external audit requirement is the most significant difference between the requirements of SOX and the Canadian SOX.

52.2 WHAT IS REQUIRED?

The CEO and CFO will be required to certify in their annual certificates that they have evaluated the effectiveness of the issuer's internal controls over financial reporting as of the end of the financial year. They will also be required to verify that, based on their evaluation, they have caused the issuer to disclose in its annual MD&A that their conclusions about the effectiveness of internal controls over financial reporting as of the end of the financial year. It is important to note that this disclosure will include a description of the process for evaluating the effectiveness of the issuer's internal controls over financial reporting and the conclusions about the effectiveness of internal controls over financial reporting as of the end of the financial year.[3]

There are a number of models being applied in Canadian companies to provide a standard approach to assess the effectiveness of the internal controls including:

- CoCo, a model issued by the Criteria of Control Board (CoCo), a body of the Canadian Institute of Chartered Accountants (CICA)
- COSO, a model developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- COBIT, an IT governance tool developed by the Information Technology Governance Institute (ITGI) that helps an organization focus its information technology in support of overall business objectives

The internal reporting requirements of MI 52-109 apply to all reporting issuers in Canada. The earliest that these requirements will apply is in respect of financial year ending on or after December 31, 2007.

The Standards for the Professional Practice of Internal Auditing published by the Institute of Internal Auditors defines a control as "any action taken by management, the board and other parties to enhance risk assessment and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved."

52.3 CoCo CONTROL MODEL[4]

CoCo defines control as comprising "those elements of an organization (including its resources, systems, processes, culture, and tasks) that, taken together, support people in the achievement of the organization's objectives."

The CoCo control model is based on four interrelated elements, as shown in Exhibit 52.2.

A person performs a task, guided by an understanding of its purpose (the objective to be achieved) and supported by capability (information, resources,

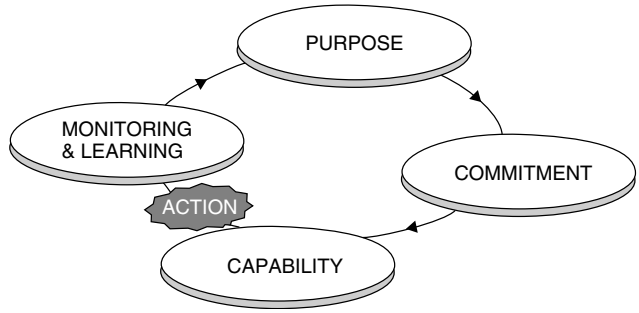


EXHIBIT 52.2 CoCo Model

supplies, and skills). The person will need a sense of commitment to perform the task well over time. The person will monitor his or her performance and the external environment to learn about how to do the task better and about changes to be made. The same is true of any team or work group. In any organization of people, the essence of control is purpose, commitment, capability, and monitoring, and learning. These four elements include a total of 20 criteria.[5]

Purpose: These criteria provide a sense of the organization's direction. They address its objectives, risks and opportunities, policies, planning and performance targets, and indicators. The components include:

P1 Objectives should be established, communicated, and prioritized to provide direction. A mission, vision, and strategy should be established toward an organization's overall objectives.

P2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed on an ongoing basis so that an organization can react to changes in an appropriate and timely manner. Risk assessment should be considered to estimate the likelihood of an event and the significance of its consequences so that appropriate policies and processes can be developed to manage them.

P3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated and practiced so that people understand what is expected of them and the scope of their freedom to act.

P4 Plans to guide efforts in achieving the organization's objectives should be established and communicated. These plans translate objectives and risk assessments into strategies, action plans, and operating and financial targets. It is a continuous process, and plans should not be static.

P5 Objectives and related plans should include measurable performance targets and indicators. The performance indicators can be used to provide early warning if targets have been exceeded or have not been met.

Some of the sample questions that an organization will use to assess the understanding of its purpose throughout the organization include:

- Do we clearly understand the mission and vision of the organization?
- Do we understand our objectives, as a group, and how they fit with other objectives in the organization?
- Does the information available to us enable us to identify risk and assess risk?
- Do we understand the risk we need to control and the degree of residual risk acceptable to those to whom we are accountable for control?
- Do we understand the policies that affect our actions?
- Do we set manageable performance targets?

Commitment: These criteria provide a sense of the organization's identity and address its ethical values, human resource policies, authority, responsibility and accountability, and mutual trust. The components include:

CO1 Shared ethical values, including integrity, should be established, communicated, and practiced throughout the organization. These provide a guide for individual, group, or team decision making, action, or policy.

CO2 Human resource policies and practices should be consistent with an organization's ethical values and with the achievement of its objectives.

CO3 Authority/responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people. Clearly defined authority, responsibility, and accountability help ensure that qualified individuals make critical decisions.

CO4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives. Mutual trust supports the flow of information that people need in order to make decisions and take action. Open communication both creates and depends on trust, and a high level of trust encourages sharing of information.

Some of the sample questions that an organization will use to assess its sense of commitment to ethical values and integrity include:

- Are our principles of integrity and ethical values shared and practiced?
- Are people rewarded fairly according to the organization's objectives and values?
- Do we clearly understand what we are accountable for, and do we have a clear definition of our authority and responsibilities?
- Are critical decisions made by people with the necessary expertise, knowledge and authority?
- Are levels of trust sufficient to support the open flow of information and effective performance?

Capability: These components provide a sense of the organization's competence. They deal with knowledge, skill and tools, communication processes, information, coordination, and control activities.

CA1 People should have the necessary knowledge, skills, and tools to support the achievement of the organization's objectives. There should be the right match of people with the tasks to be performed along with the necessary skills and capabilities, which can be assessed through the establishment of requirements and training.

CA2 Communication processes should support the organization's values and the achievement of its objectives. For control to be effective, an organization should have a communication process capable of supporting open communication of timely, relevant, and reliable information. Two-way communication helps to ensure that communication processes are flexible and responsive, and communicating the views of the most directly affected by decisions are key to the success of implementation.

CA3 Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.

CA4 The decisions and actions of different parts of the organization should be coordinated. Since larger organizations are typically complex with varying departments and divisions, decision and actions should require coordination to achieve objectives as a whole. Coordination improves integration, consistency, accountability and limits autonomy.

CA5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the interrelatedness of control elements. Control activities are routines established to provide assurance that processes operate as designed and meet the requirements of the organization's policies.

Some of the sample questions that an organization will use to assess its capability component include:

- Do we clearly have the right people, skills, tools, and resources?
- Is there prompt communication of mistakes, bad news, and other information to people who need to know, without fear of reprisal?
- Is there adequate information to allow us to perform our tasks?
- Are our actions coordinated with the rest of the organization?
- Do we have the procedures and the processes to help ensure achievement of our objectives?

Monitoring and Learning: These components provide a sense of the organization's evolution. They entail reviewing internal and external environments, monitoring performance against targets, challenging assumptions, reassessing information needs and systems, establishing follow-up procedures, and assessing the effectiveness of control.

ML1 External and internal environments should be monitored to obtain information that may signal a need to reevaluate the organization's objectives and controls. Monitoring the external environment can provide valuable information on the state of the internal environment, and to a large extent, managers can initiate or control changes to the internal environment. Information gained through monitoring environments may signal a need to reevaluate the organization's objectives or other aspects of the organization.

ML2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans. To monitor performance, there must be timely and reliable information made available on operating results.

ML3 The assumptions behind an organization's objectives should be periodically challenged. If an organization's assumptions are incorrect or outdated, control may be ineffective, and periodically changing an organization's assumptions can be the key to effective control.

ML4 Information needs and related information systems should be reassessed as objectives change and as reporting deficiencies are identified.

ML5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs, enabling control to remain effective. For change to be effective, information such as the results of control assessments must be communicated to those who can authorize change.

ML6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.

Some of the sample questions that an organization will use to assess its monitoring and learning component include:

- Do we review the internal and external environment to see whether changes are required to objectives and controls?
- Do we monitor performance against relevant targets and indicators?
- Do we challenge the assumptions behind our objectives?
- Do we receive and provide information that is necessary and relevant to decision making?
- Are our information systems up to date?
- Do we learn from the results of monitoring and make continuous improvements to control?
- Do we periodically assess the effectiveness of control?

The criteria that need to be addresses included both hard and soft controls. The hard controls, which are more easily measured or analyzed, may include such elements as organizational structure, formal processes, and policies and procedures. The soft controls include characteristics such as tone at the top, trust, shared values, and commitment. The soft controls tend to be based on observation because they are based on intangibles and are behavior-based.

52.4 COMPARISON OF CoCo TO COSO[6]

There are three main differences between the American COSO and Canadian CoCo framework on internal controls. The differences between the two internal control frameworks can be found in the definition and the scope, the underlying concepts, and the judgment of effectiveness.

(a) DEFINITION AND SCOPE. COSO defines internal control as a process, affected by an organization's directors, managers, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

CoCo defines control as the elements of an organization (including its resources, systems, processes, culture, structure, and tasks) that, taken together, support people in the achievement of the organization's objectives. It defines the following categories of objectives:

- Effectiveness and efficiency of operations
- Reliability of internal and external reporting
- Compliance with applicable laws and regulations and internal policies

Consistent with its definition, CoCo includes the scope of control for some particular aspects of management that COSO excludes such as objective setting, strategic planning and risk management, and corrective actions. CoCo does exclude decision making from the scope of control.

(b) UNDERLYING CONCEPTS. CoCo is explicit about some concepts that are not addressed in COSO. These are:

- Control includes the identification and mitigation of the risk failure to maintain the organization's capacity to identify and exploit opportunities.
- Control includes the identification and mitigation of the risk of failure to maintain the organization's resilience—its capacity to respond and adapt to unexpected risks and opportunities, and to make decisions on the basis of telltale indications in the absence of definitive information.
- CoCo includes two criteria not explicitly addressed in COSO. They relate to mutual trust between people and the periodic challenge of assumptions. In addition, the concept of monitoring in the CoCo guidance includes monitoring of the operating performance of the organization. COSO's discussion of monitoring could be interpreted as focused on monitoring of specific control activities.

(c) JUDGMENT OF EFFECTIVENESS. COSO addresses this as follows: "Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:

1. They understand the extent to which the organization's operations objectives are being achieved.
2. Published financial statements are being prepared reliably.
3. There is compliance with applicable laws and regulations.

Determining whether a particular internal control system is effective is a subjective judgment resulting from an assessment of whether five components (control environment, risk assessment, control activities, information and communication, and monitoring) are present and functioning effectively. Their effective functioning provides the reasonable assurance regarding the achievement of one or more of the stated categories of objectives. Thus, these components are also criteria for effective internal control.

(d) CoCo DIFFERS IN THREE IMPORTANT RESPECTS

1. The judgment of effectiveness in CoCo is made in relation to a specific objective, not a category of objectives.
2. CoCo asks that an assessment of the effectiveness of control be made against 20 specific criteria. COSO asks that assessment be made for each of five components, and provides illustrative issues to consider for each component. All of COSO's issues to consider are addressed directly or indirectly within the CoCo document, except perhaps the following:
   - Receptivity of management to employee suggestions of ways to enhance productivity, quality, or other similar improvements
   - Extent to which personnel, in carrying out their regular activities, obtain evidence as to whether the system of internal controls continues to function
   - Extent to which outside parties have been made aware of the entity's ethical standards
   - Extent to which training seminars, planning sessions, and other meetings provide feedback to management on whether controls operate effectively
   - Appropriateness of the level of documentation (of an evaluation)
3. CoCo includes the following definition of effective control: Control is what makes a municipality reliable in achieving its objectives. Control is effective to the extent that it provides reasonable assurance that the municipality will achieve its objectives.

52.5 CONCLUSION

There is not a specific defined approach to address compliance with MI 52-109 in Canada. An organization should evaluate the various control assessment frameworks available and select one or combine those areas of each of the available frameworks that best meets its needs. Ultimately, the objective of Bill 198 is to ensure increased accuracy in financial reporting. In so doing, companies are able to better manage and mitigate risk within the organization, and achieve higher levels of corporate governance.

Notes

1. OSC Multilateral Instrument 52-109—*Certification of Disclosure in Issuers' Annual and Interim Filings*.
2. OSC Multilateral Instrument 52-108—*Auditor Oversight* and OSC Multilateral instrument 52-110—*Audit Committees*.
3. CSA Notice 52-313—Status of Proposed MI 52-111 *Reporting on Internal Control over Financial Reporting*.
4. "CoCo's Control Framework," editorial by Nelson Luscombe, *CA* Magazine, December 1995.
5. "Enhancing Management Involvement with Internal Control," Financial Management Capacity Building Committee (FMCBC), August 2005, Appendix III: CoCo's Internal Control—Integrated Framework—Comparison of CoCo to COSO.
6. Ibid.

CHAPTER 53

CORPORATE GOVERNANCE: CHINA

Anthony Tarantino, PhD

53.1 INTRODUCTION

China has become one of the most watched, feared, and admired nations in the world. By the middle of this century, it is estimated China's economy will be substantially larger than the U.S. economy. Critics condemn human rights abuses and China's growing geopolitical influence. (Ironically, the critics fearful of Chinese political and military expansion are projecting Western traits on a country that suffered centuries of foreign intrusions and exploitation yet has never mimicked Western-style imperialism.) Admirers note that China has transformed like no other society in modern history and consistently enjoys the world's highest growth rate with its unique blend of central planning and market driven enterprises.

Both admirers and critics realize that China is an economic powerhouse. China's gross domestic product (GDP) has increased roughly sixfold since 1978 as compared to a twofold increase for the United States over the same period. Projections from PricewaterhouseCoopers show China surpassing the United States as the world's largest economy by 2050 as measured by GDP in terms of purchasing power parity (PPP). (See Exhibit 53.1.)

To put this incredible transformation in perspective, we offer the story of a man named Mr. Keren Cui and his experiences during the Great Proletarian Cultural Revolution (1966–1976), a period when notions of free speech and market-driven corporate governance were either unknown or treated with great

	GDP PPP with the U.S. = 100				
	2005		2050		2005 to 2050
Nation	Rate	Rank	Rate	Rank	Change vs. U.S.
China	76	2	143	1	**67**
U.S.	100	1	100	2	N/A
India	30	4	100	2	**70**
Brazil	13	9	25	3	**12**
Japan	32	3	23	4	**(9)**

Source: PricewaterhouseCoopers, 2005.

EXHIBIT 53.1 PROJECTIONS OF GDP PPP CHANGE, CHINA VERSUS OTHER COUNTRIES

mistrust. The terms and concepts of *corporation* and *legal person* did not exist at this time. As Mao attempted to rekindle the revolution, open discussion or resistance to the Red Guard revolutionaries was met with harsh treatment. Mr. Cui saw the China he admired being torn apart and dared to speak out against the breakdown in civility and human rights. He was arrested for his transgressions against the revolution. To make an example of him, Mr. Cui was hung by his wrists for the day from a tree while his captors beat him in a public square.

During the Cultural Revolution schools taught only from Mao's collected works. As a result, an entire generation suffered from large gaps in their education. Mr. Cui read Mao every day during his imprisonment, as it was the only material available to him and a means for him to pass the time. His wrist injuries were so severe that he could only turn the pages with his tongue. He spent a year in jail without due process or a trial and then was released in 1969. His wife, a schoolteacher, was forced out of her job and sent to the countryside to cook for a school. Their two oldest children learned virtually nothing in school for at least six years; they spent their time reading Mao and other political propaganda.

Today Mr. Cui is retired and lives with his wife of 47 years. The scars on his wrists are his most vivid reminder of the dark days. When asked about the changes in the past 35 years, Mr. Cui says he believes there has been great progress. He feels free to express his opinions and to travel anywhere in the country. He now enjoys online investing in the Shenzhen and Shanghai stock markets. Improvements in corporate governance give him confidence that his investments are better protected than in the early days of corporations, when bankruptcies were more commonplace.

There were some good things that came out of the Cultural Revolution such as the birth of his youngest daughter, who is a successful American sales executive and married to the author of this chapter. His other children are successful as well, working for Chinese government agencies.

Mr. Cui is not alone in his enthusiasm for investing in China's booming economy.

The investor environment resembles that of the United States in the 1920s and 1990s, when it was commonplace for middle- and working-class people to buy stocks on high margins with little concern for downside risks. When stocks fell dramatically, investors could not cover their losses, which sparked the market crash of 1929 and dot-com meltdown of the 1990s.

Chinese regulators do not want to see U.S. history repeat itself in their country on their watch.

Chinese investors are mortgaging their homes and borrowing against their credit cards to get a piece of the action. The Shanghai Stock Composite Index increased by 130 percent in 2006, making China's stock markets among the best-performing in the world. China is also the home for some of the hottest initial public offerings (IPOs). The lure of high stock growth has attracted many new investors, and like Mr. Cui, they are trading online—opening 90,000 accounts per day, which is 35 times the pace of the prior year. The bulk of the stock trading is by local Chinese investors, who represent a majority of the market's capital. China now has over 80 million individual investment accounts and a $1 trillion market capitalization in its two exchanges. This is still small when compared the NYSE's $26 trillion levels, but does rank third in Asia after Japan and Hong Kong.[1]

China has gone through a boom-and-bust cycle as recently as 2001, when stocks peaked and then tanked for the next four years. Ironically, many investors blamed their losses on the government because of its endorsement of markets just weeks before the collapse. The 1990s were a tumultuous period of stock fever with investors rioting to get a piece of hot IPOs. The lack of regulations and oversight led to a series of scandals and stock manipulations that badly shook investor confidence. A 2004 poll showed the troubled stock market as the public's major concern.[2]

Premier Wen Jiabao acknowledged the problems in a 2004 speech, which led to a variety of reforms. The reforms have paid off with the markets rebounding form eight-year lows to all-time highs in 2006. Stocks are trading at bubblelike price-earnings ratios, or above 30 times earnings. As a comparison, stocks on the Hong Kong exchange trade below 20 times earnings.

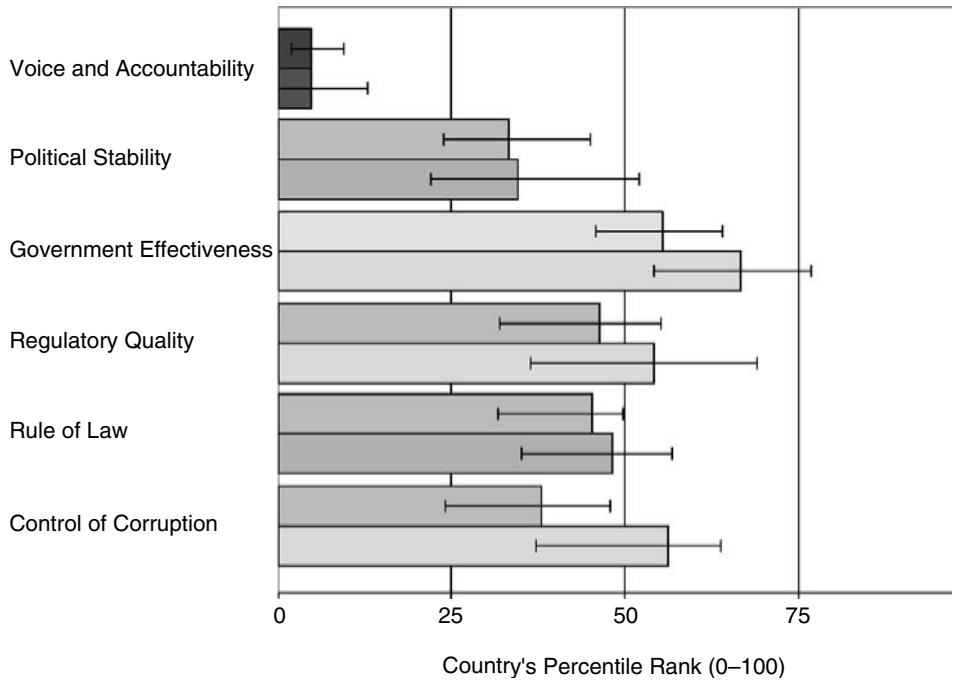
The booming economy and exchanges have created a new class of multi-millionaires. *Forbes* magazine listed the 40 wealthiest people in China for 2006. Reflecting the booming economy, it takes a minimum wealth of $514 million to make the list, an increase of over 35 percent from the 2005 minimum. The combined wealth of the top 40 increased by about 50 percent to $38 billion from the previous year. There are two women on the list, and the great majority of the 40 have greatly benefited from China's new corporate model, with their fortunes coming from the value of their companies' stock.[3]

So much for the ghosts of the Cultural Revolution.

53.2 WORLD BANK RATINGS FOR SIX ELEMENTS OF GOVERNANCE

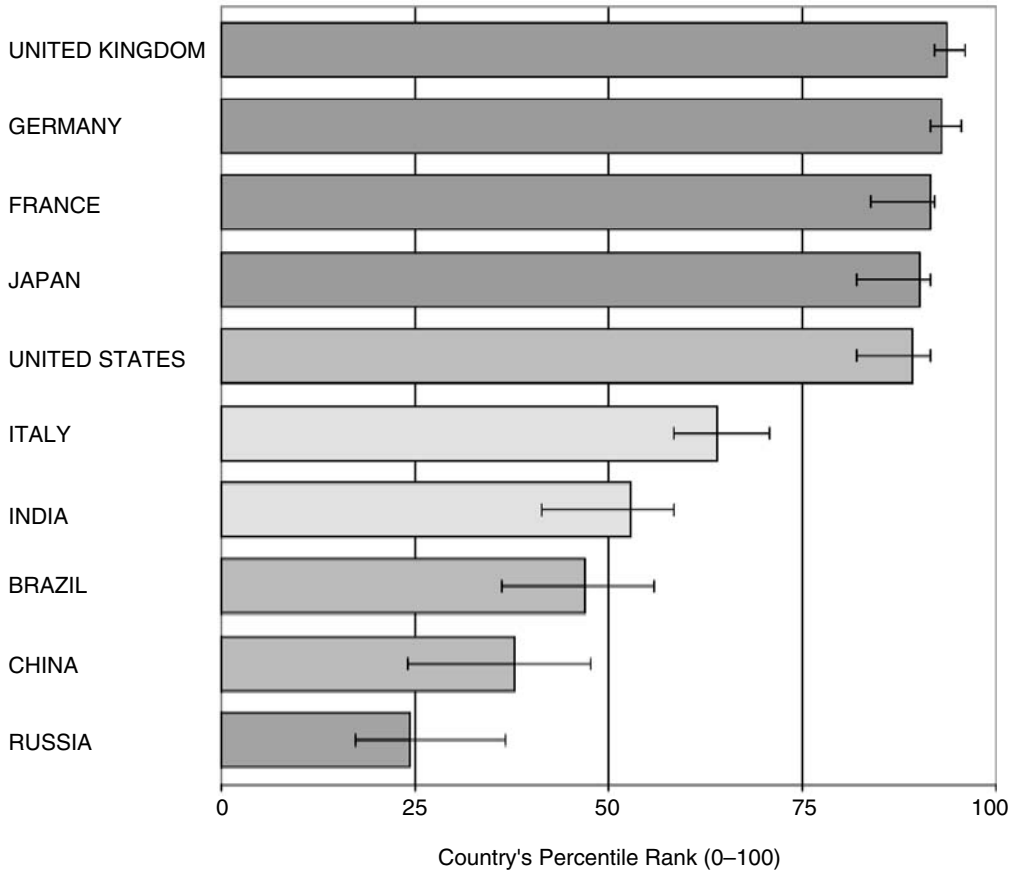
The World Bank measures over 200 nations on six elements of compliance. The latest ratings are for 2006 and represent one of the most viable means of comparing nations. The World Bank correctly assumes that corporate governance does not exist in a vacuum and can only prosper with factors that exist outside of corporations: political stability, lack of violence, government effectiveness, rule of law, corruption control, voice and accountably (freedom of religion, press, and speech). (See Exhibit 53.2.)

The results show no significant improvement in five elements over nine years: voice and accountability, political stability/no violence, government effectiveness, regulatory quality, and rule of law. Of even greater concern is the major deterioration in controlling corruption. The next graph (Exhibit 53.3) compares China's control of corruption against the leading GDP nations. The Chinese are not alone among major economies in their lack of progress. As a comparison, the United States has also lost ground in voice and accountability as well as political stability/no violence, and has not made progress in any of the other four areas.



Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 53.2 WORLD BANK GOVERNANCE RANKINGS: SIX ELEMENTS FOR CHINA 2006 AND 1996 (TOP-TO-BOTTOM ORDER)

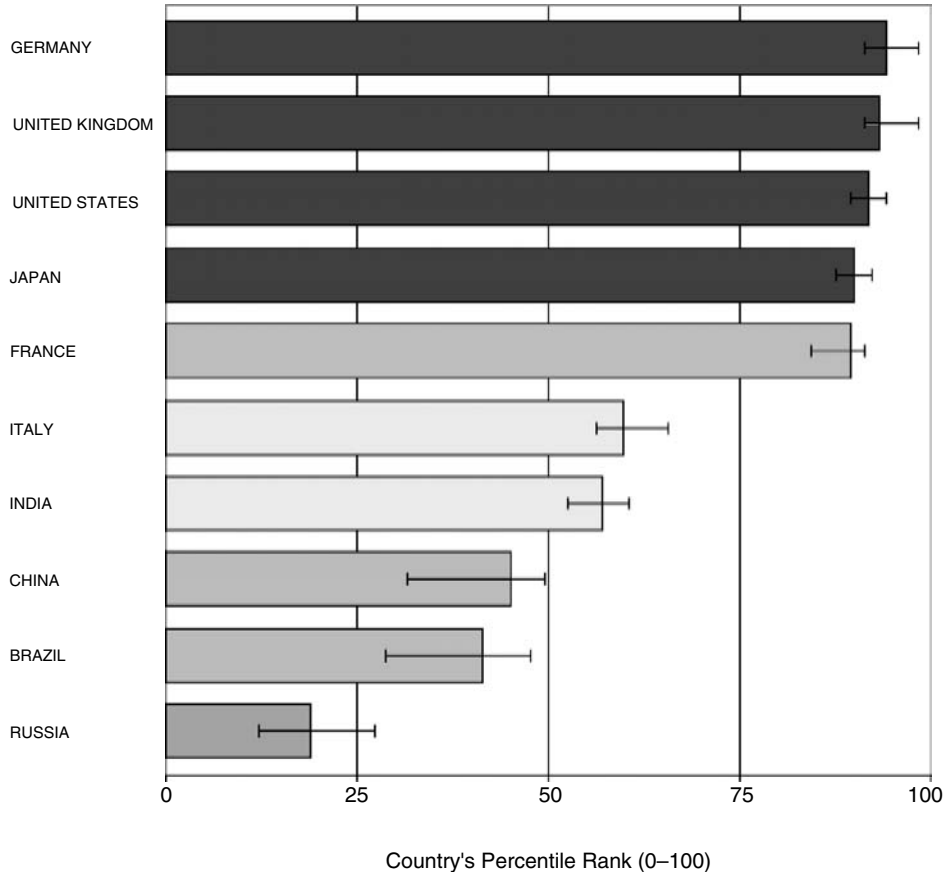


Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 53.3 WORLD BANK GOVERNANCE RANKINGS: CONTROL OF CORRUPTION FOR CHINA AND THE MAJOR GDP COUNTRIES

In Exhibits 53.3 and 53.4, China leads only Russia in these two critical metrics of governance and scores less than half the rate of the leading economies.

With projections that China will be the world's largest economy and that India will be tied with the United States as the world's second largest economy by 2050, it is interesting to compare the two Asian giants. (See Exhibits 53.5 and 53.6.) India has a long history of British political, economic, and business influences, and is the world's largest democracy. China is still a Communist nation and less than 12 years into its acceptance of Western-style corporations. So it is somewhat surprising that India does not have a larger lead over China. In the area of regulatory quality, China ranks about the same as the average for Asian nations and ahead of the average for South Asian nations.

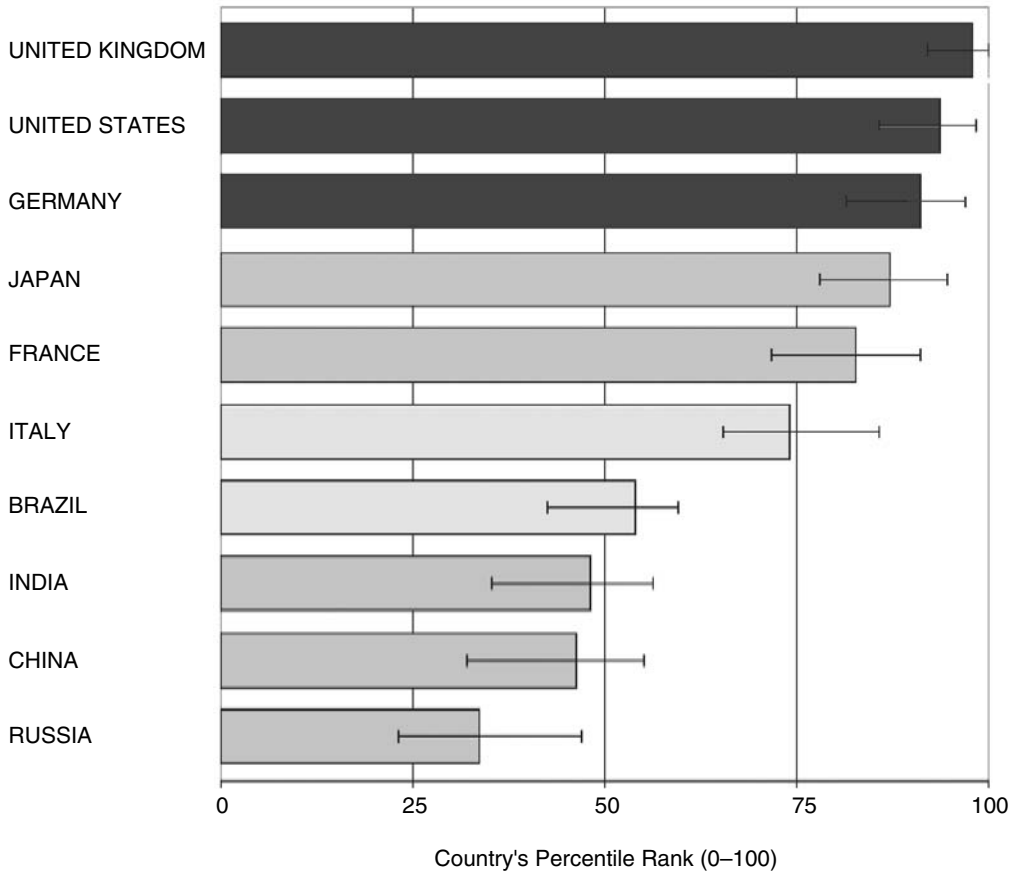


Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 53.4 WORLD BANK GOVERNANCE RANKINGS: RULE OF LAW FOR CHINA AND MAJOR GDP COUNTRIES

53.3 TRANSITION FROM STATE-OWNED ENTERPRISES (SOES) TO CORPORATIONS

To understand corporate governance in China, it is helpful to summarize the evolution of state-owned enterprises (SOEs). Since the 1949 revolution, SOEs have controlled business activities. SOEs have evolved from a model (1950–1984) in which the government controlled all rights to property ownership and management, to a transitional model (1984–1993) where these rights were shared between the government and management, to today's contracting model (1993 to present) where each business is responsible for its own profits and losses while being governed by Western-style corporate codes of conduct and accounting standards—the model found in most market-based economies.

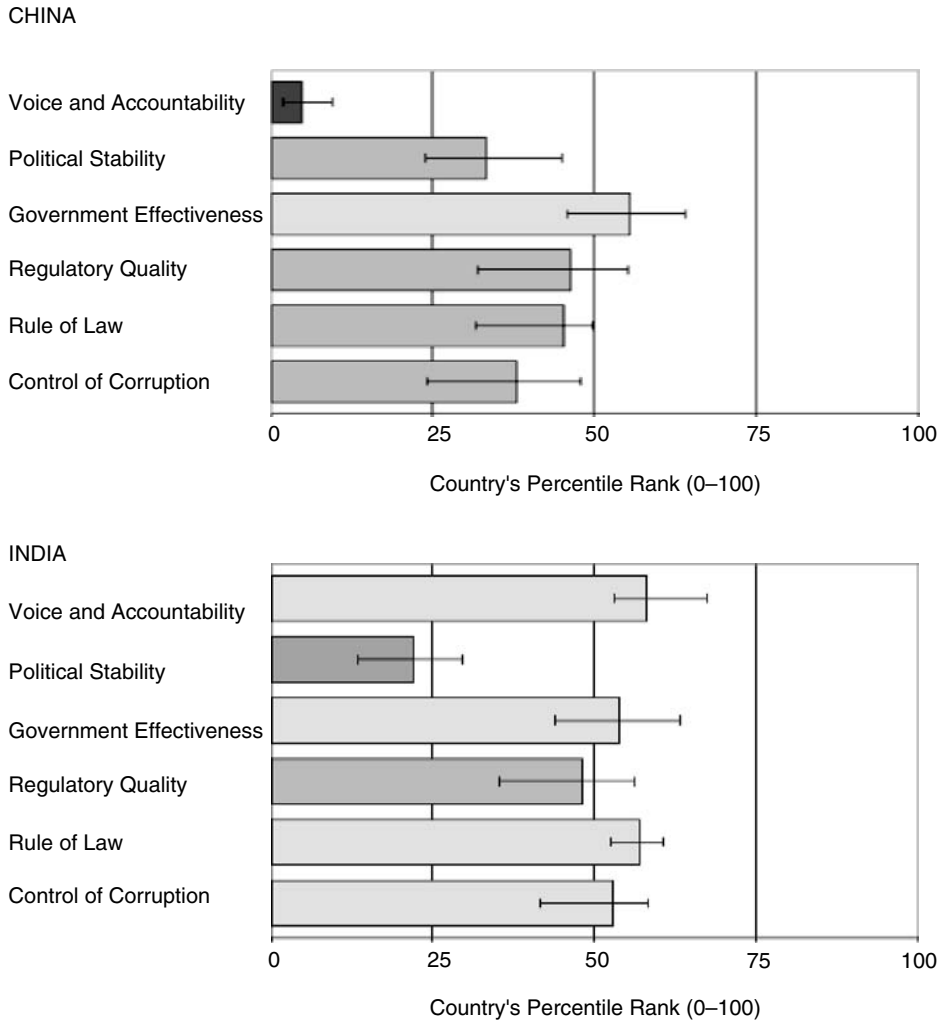


Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 53.5 WORLD BANK GOVERNANCE RANKINGS: REGULATORY QUALITY FOR CHINA AND LARGE GDP NATIONS

State Ownership and Management Model (1950s to 1984). Government ownership and management control were seen as necessary to protect state property. The lack of independence, rewards, and market forces had the obvious effect of depressing growth and efficiency. Most SOEs were simply regarded as factories without any corporate charter or structure. Factory managers were only accountable to government officials, typically to meet central planning objectives and with little regard for financial performance. Employees were given long-term job security, housing, benefits, and pensions, so there were few incentives to challenge the status quo.[4]

Transitional Model (1984 to 1993). The transitional model of SOE governance is also known as the state-creditor's rights model, or the contracting



Source: Kaufmann, Daniel, Kraay, Aart and Mastruzzi, Massimo, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 53.6 WORLD BANK COMPARISON OF CHINA (TOP CHART) AND INDIA (LOWER CHART)

model. This model was dominant until the enactment of the Chinese Corporate Law in 1993, and was seen as a means to expand profits and production. The transitional model introduced the radical notion of SOE responsibility for profits and losses. With the responsibility came greater authority and the beginnings of the separation between management rights and state ownership. The transactional model also introduced the legal concept of the SOE as a legal entity. In order to codify this reform process, the State-Owned Industrial Enterprises Law, known

as the SOEs Law, was enacted in 1988. The SOE Law included the following requirements:

- The factory manager has management responsibility over the enterprise.
- The factory manager is the legal representative of the enterprise.
- The local Communist Party organization assures the SOE follows the party's guiding principles and policies.
- The SOE can practice democratic management through employee congresses and trade unions.[5]

The transitional model and its contracting process resulted in a greatly diminished level of governmental intervention in SOE operations and the SOE's retention of a portion of their profits. As might be expected, the SOE transitional scheme failed, as have most all similar schemes in which governments overly intervene in business enterprises. This led Chinese officials to look at the capitalist West for a solution—market-driven enterprises based on Western corporate organizations and governance.

The Modern Corporate Model (1993–Present). In 1992 China's great leader, Deng Xiaoping, called for a transition to a market-driven economy, marking remarkable and fundamental change from the founding principles of the Chinese Communist revolution. As part of the movement toward a market economy, China would create Western-style corporations with their accompanying legal and regulatory systems of corporate governance. This required restructuring many traditional SOEs, now known as SOE-corporatized corporations. Under the new model, shareholder rights are better defined than in the past. Transparency, efficiency, and accountability are improved along the lines of Western corporations.

53.4 THE CORPORATE LAW OF 1993–2006

To support this dramatic change, the Corporate Law of 1993 was enacted and has been revised periodically through 2006.[6] The Corporate Law defined three distinct types of corporate entities:

1. *Wholly state-owned corporations* are limited liability corporations created by the government or investment institutions with state authorization. Modern SOEs are governed by the Corporate Law of 1993 and the SOE Law of 1988. SOEs remain a pillar of the Chinese economy, but decades of centralized planning have resulted in major financial difficulties for thousands of these organizations. (As of 1998, there were 238,000 noncommercial SOEs, according to the Ministry of Finance.)
2. *Closely held corporations* enjoy reduced governance standards due to their limited number of shareholders and limited capitalization. They are not typically required to set up a board of directors. There are special provisions for foreign-invested firms, but these are expected to change with China's joining the World Trade Organization (WTO).

3. *Publicly held corporations* are also known as joint stock limited companies in which all the capital is divided into equal shares, and thus shareholders' financial exposure is limited to the number of shares they own.

The Corporate Law of 1993 also introduced two legal positions found in Western corporations:

1. The chairman of the board of directors (chair), who acts as the corporation's sole legal representative, exercises powers given him or her by the board, chairs shareholder and board meetings, examines board resolutions, and signs corporate issued shares and bonds.
2. The chief executive officer (CEO) acts as the corporation's agent and employee with the daily operations of the business. He or she is accountable to the board, which has authority over his or her employment status and compensation.

Both closely held and publicly held corporations are required to maintain three governing bodies:

1. *The board of directors.* Unlike Western boards, Chinese boards are not specifically empowered to appoint committees to oversee compensation, nominations, and audit. In practice, only overseas listed corporations maintain such committees.
2. *The shareholders acting as a body at the general meeting.* Although the shareholders' general meeting is supposed to be the supreme authority in corporate governance, they are often more of a rubber stamp to corporate activities. Shareholder majority votes can determine corporate policies, elect and remove directors, set board member compensation, elect shareholder supervisors, and review and approve director reports, budgets, and strategic plans, including mergers and acquisitions.
3. *The board of supervisors.* The Chinese system of board of directors and supervisors is not based on the two-tiered German system in which a board of supervisors oversees the activities of a board of directors. In the Chinese model the board of directors and supervisors are on the same level and subject to shareholder actions.

53.5 SUGGESTED IMPROVEMENTS IN THE CORPORATE LAW

There are many areas of the Corporate Law that need improvement. This is well understood within and outside of China. Here is a summary of some of the major improvements that are under discussion:

Repeal of the SOEs Law: Since the SOEs Law of 1988 creates confusion and conflicts with the Corporate Law of 1993, it should be repealed. All SOEs should be governed by one unified corporate law.

Reduce Government Involvement in SOEs: Government officials' meddling and solicitation of fees, fines, and donations cripple the effectiveness of any organization.

Reduce Communist Party Involvement in SOE Corporations: In the ultimate oxymoron (Communist Party board member), it is hard to see how Communist Party participation in a market-based corporation can ever be productive.

Improve Shareholder Meetings: In many Western nations, shareholders are given only limited powers in running corporations. In China shareholders are considered the ultimate source of authority, and all board powers are derived from shareholders. This corporate governance philosophy mimics the political governance philosophy expressed in the Chinese Constitution. In reality, shareholders rights need to be strengthened to improve corporate management and operations.

Improve the Role of the Board of Directors: Corporate boards will need to take greater responsibility to improve the nimbleness, efficiency, and effectiveness of corporations. It is not practical to rely on shareholder meetings. The process is too time consuming and ineffective.

Expand the Use of Committees of the Board of Directors: With the exception of overseas listed corporations, Chinese corporations do not typically appoint specialized committees to oversee such functions as audit, compensation, and nominations. These committees, made up experts in their fields, are essential in improving corporate governance.

Increase the Independence of Corporate Boards: There are no requirements that mandate the independence of board members. Independence brings checks and balances, essential in improved governance. Independence is no panacea, though, in that the Enron scandal occurred under a board with a large majority of independent members.

Improve Controls over Directors and Executives: Many SOE corporate failures in the 1990s resulted from abuses and lack of competence by directors and corporate executives. There is no assumption of a fiduciary relationship between directors and executives and the corporation as exists in the West. Ironically, China's great Confucian philosophy may be the world's earliest role model for the fiduciary relationship between those in power and those they govern. Communist officials are also assumed to have a fiduciary relationship with their comrades. So the lack of a fiduciary relationship in corporations is disappointing and a little surprising.

Increase Board Compensation: Chinese corporate board members are typically compensated at rates equivalent to $4,000 to $10,000 U.S. dollars or euros. The poor compensation is an open invitation to corruption. In America there is an old joke about not bothering to pay a bartender a decent wage since they are going to pocket so much of the bar proceeds. Increasing board compensation is the only viable means to lower the temptations of corruption and bribery.[7]

Beware of Stock Options: Chinese executives are renewing their interest in stock options as the economy booms. In spite of the growing U.S. scandals, government regulators are becoming more receptive to them as well. In theory, this type of derivative arrangement makes good sense—managers are rewarded for the growth of their company's stock value.[8] Unfortunately, U.S. history is

likely to repeat itself. Managers will make shortsighted decisions to force up the value of stocks or play accounting tricks such as backdating the issue dates. The U.S. scandals continue to spread and now include well over 100 corporations. Many U.S. companies have fired executives and restated earnings going back several years. This is a painful journey that Chinese business leaders and government regulators can avoid with fair compensation and bonuses tied to long-term corporate goals.

53.6 CHINA'S SHANGHAI AND SHENZHEN STOCK MARKETS

China's two stock exchanges are immature and small when compared to other leading economic powers, but there is a great deal of interest among individual Chinese investors propelling their growth.

The Shanghai Stock Exchange was reestablished in 1990. Ironically and possibly an omen of things to come, the Shanghai exchange was the world's third largest stock exchange in the early twentieth century. In the same year, a second exchange was established in Shenzhen, a short train ride from Hong Kong. Shenzhen is a truly remarkable city transformed from a small village into a booming center of commerce in less than a generation. The two exchanges reached a total capitalization of $900 billion in 2006. This equals 30 percent of GDP and is very small by Western and Japanese standards, which are typically well over 100 percent. Traditionally, the large majority of stocks represent SOEs restricted by state ownership and nontradable shares, but most listed companies are in the process of making stocks fully tradable.[9]

The growth of the Chinese exchanges have been hampered by a regulatory environment that lags the leading economies. The China Securities Regulatory Commission (CSRC) has made some important steps toward reforms but is hampered by continuing state instance to prop up weak SOEs, which would be allowed to fail in a market-driven economy. Bringing CSRC staff up to the needed levels of expertise will be a challenge as well, but China has shown a remarkable ability to quickly adapt and master Western capitalist concepts. The CSRC recently raised the bar by requiring all security brokerages to file audited financial results going back to 2006. The results are available at the brokerage web sites as of June 2007.

Notes

1. James T. Areaddy, "Stock Frenzy in China Stokes Official Concern: Investors Pile In, Using Homes as Collateral, Tapping Credit Cards," *Wall Street Journal*, January 30, 2007, A1.
2. Ibid.
3. Russel Flannery, "China's 40 Richest," Forbes Asia 67.2, Issue 19, November 2006.
4. Cindy A. Schipani and Liu Junhai, "Corporate Governance in China: Then and Now," *Columbia Business Law Review*, 2002, 1–69.
5. Ibid.

6. See Wu Kun, "Understanding Revisions to the Company Law: A Comparison of the New with the Old," *Asia Business Intelligence*, November 21, 2006; Seung Chong, "The A to Z Guide to Chinese Company Law," *International Financial Law Review*, April 1, 2006.
7. Schipani and Junhai, "Corporate Governance."
8. Richard Meyer, "In China, Stock Options Finally Taking Root," *Compliance Week*, November 28, 2006.
9. *Economist* Intelligence Unit, "China: Financial Services," *Economist*, January 2007.

CHAPTER 54

CORPORATE GOVERNANCE: FRANCE

Anthony Tarantino, PhD

54.1 INTRODUCTION

The French model of corporate governance has undergone a major transformation in the past ten years. This was facilitated by the following developments:

Foreign Investors: The CAC 40 is named after the Paris Bourse's early automation system called the Cotation Assistée en Continu, or Continuous Assisted Quotation. It is the leading stock market index in France, consisting of a capitalization-weighted measure of the 40 highest capitalized corporations. The CAC-40 is a subset of the larger SBF 250 (Societe des Bourse Francais). Ironically, about 45 percent of CAC 40 shares are now owned by foreign investors. The leading investors come from Germany, Japan, the United States, and Britain. Many of these investors represent UK and US pension funds and a majority of CAC 40 employees live outside of France. The foreign ownership of CAC 40 and other leading French firms represents a major shift in ownership over the last ten years. In the past ownership was concentrated in domestic owners who were more friendly to company management and not as demanding in terms of corporate governance.[1]

Corporate Diversification: Larger French companies have dismantled much of their conglomerate structure in a move away from earlier policies favoring diversification into many business areas. Most larger companies, with the

exception of some family owned firms, now taken a course favoring a focus on a limited number of core competencies. As a consequence, employees of many of these companies have lost protection provided that was afforded by the subsidized nature of these businesses. Employment in these firms is not much more contingent on company performance.

Management Performance Incentives: Most French firms have implemented performance incentives for senior management. About half of CEO compensation is now variable and tied to performance. France leads the EU in paying the highest stock option packages.[2]

The mid-1990s witnessed the first major focus on corporate governance in France. This was sparked by the growing importance of foreign ownership described above and by a number of spectacular financial losses caused by unmonitored managerial initiatives such as Michelin, Paribas, Credit Lyonnais, Suez, and Union des Assurances de Paris. The initial public reaction to the concept was unlike that in the United States which had been stung by a series of scandals which shook public confidence. In France corporate governance and shareholder value concepts were typically associated with job losses as corporations put short term financial gains ahead of long term stability and employee protection.[3]

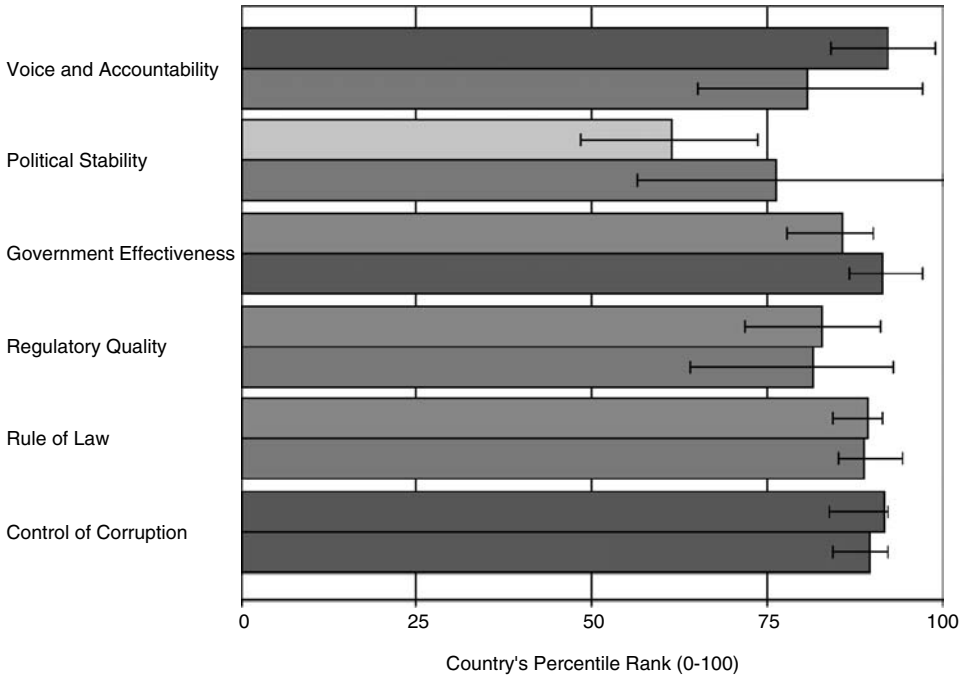
The spectacular growth of the U.S. economy in the 1990s convinced many in France of the need to change its economic system. Corporate governance to promote shareholder values came to be seen as a vehicle to access international equity capital.

This view changed with collapse of the Internet bubble and a series of major U.S. scandals. They were seen as a vindication of the French conservatism and common sense in refusing to adopt Enron-type off-balance-sheet techniques to hide losses. (Ironically, the abuse of off-balance-sheet accounting behind the Enron fiasco was not resolved by the most controversial and costly provisions of the U.S. Sarbanes-Oxley Act—Section 404.)

CAC-40 and other large firms have driven the corporate governance process with little involvement by either regulators or employees. In this way, the process has mirrored that of the industrial restructuring of the past twenty years. French companies dissolved their conglomerate organization with few employee concessions or guarantees.

54.2 CURRENT STATE OF CORPORATE GOVERNANCE

The World Bank publishes country-to-country and year-to-year evaluations covering six areas of governance. By these measures, France is a leader in Europe and globally. France ranks sixth in regulatory quality, fourth in control of corruption, and fourth in the rule of law when compared to the world's leading economies. It has declined in two categories over the past nine years—political stability/no violence and regulatory quality. (See Exhibits 54.1 to 54.4.) France's



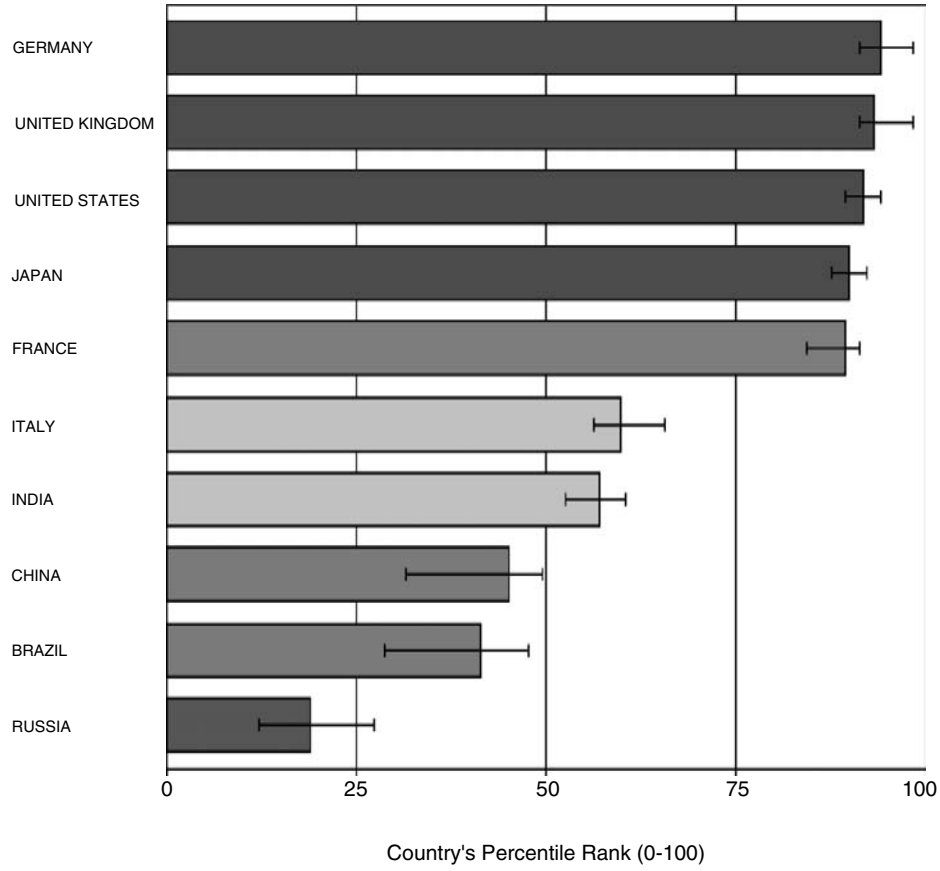
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

EXHIBIT 54.1 WORLD BANK GOVERNANCE RANKINGS: SIX ELEMENTS FOR FRANCE 2006 AND 1996 (TOP-TO-BOTTOM ORDER)

lower ranking in its regulatory quality and decline in political stability over the last nine years should be seen as the major challenge and opportunity to be addressed in the next few years.[4]

Much of France's progress in improving corporate governance can be attributed to the passage of the Yearly Budget Law (LSF) and NRE Law (regulating disclosure) both of which came into force in 2004. French companies are coming to realize the market benefits of improved governance, especially in the area of transparency, which will expand the adoption of the two acts. This should translate into higher World Bank ranking for regulatory quality.

According to the Heidrick & Struggles 2005 study, 100 percent of firms now have audit committees (an increase of 7 percent since 2003), but only 20 percent of audit committees are wholly composed of nonexecutive and independent directors. By comparison, 98 percent of British firms have independent audit committees. The lack of independence can also be seen in remuneration or compensation committees. While 95 percent of CAC-40 firms have such a committee, just 18 percent are entirely independent.[5]

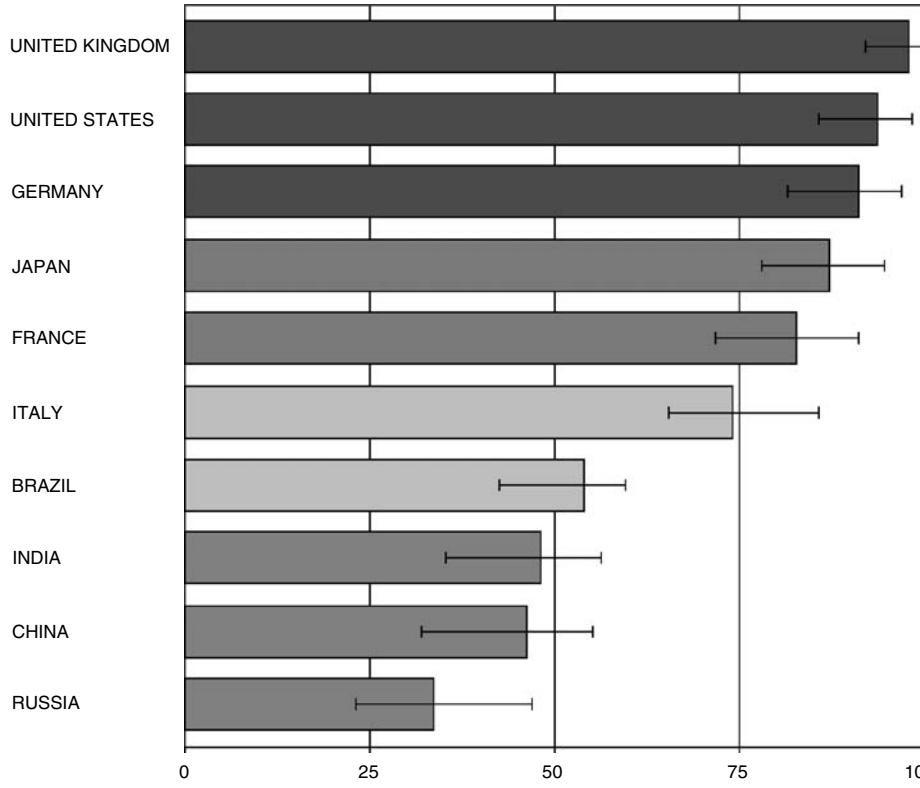


Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

EXHIBIT 54.2 WORLD BANK GOVERNANCE RANKINGS: RULE OF LAW FOR FRANCE AND MAJOR GDP NATIONS

There is better progress in nomination committees, with over 80 percent of companies now possessing one, up from 63 percent in 2003. On the down side, just 5 percent have ethics committees, compared with 22 percent for British companies.[6]

The independent oversight by boards will continue to be challenged in that only 35 percent of committee chairs are not independent, as compared with 48 percent in Europe overall. Even worse, 25 percent of companies have no independent directors on their boards. The actual independence and nonexecutive status of some of these board members is also debatable.[7] This is undermines the value a board can add by identifying weaknesses and recommending improvements in operations and financial transparency reporting. France has a way to go in terms of



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

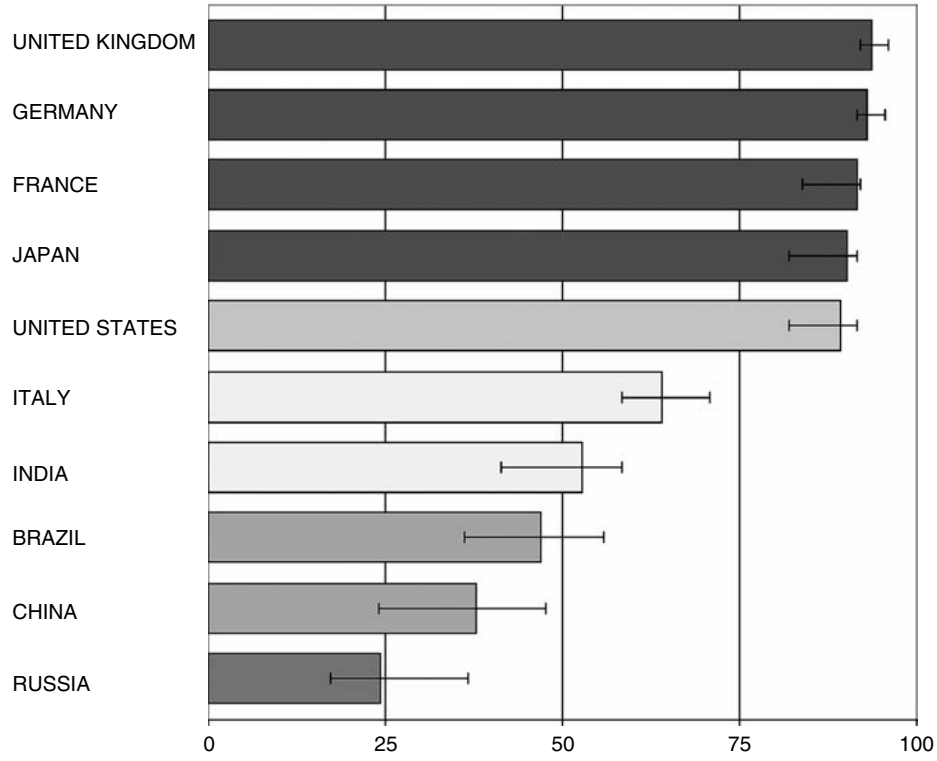
EXHIBIT 54.3 WORLD BANK GOVERNANCE RANKINGS: REGULATORY QUALITY FOR FRANCE AND MAJOR GDP NATIONS

director compensation. With an average of 35,000 euros, this puts France among the lowest in the EU and far below the 63,000 average.[8] It takes top talent to move an organization forward, and these low levels of compensation are not the way to do it.

Diversity and age remain issues in French and EU boards in general. Consistent with EU averages, women are badly under represented in board composition, at only 7 percent. French boards remain a little older than the average in the EU by two years—54.5 versus 58.2, with an average tenure about one year longer than EU averages. This situation will not facilitate the process of bringing newer and higher-quality talent to the boardroom.

54.3 MEDEF AND AFEP CONSOLIDATED CODE

French corporate governance emerged in 1995 by an initiative between two French associations: Mouvement des Entreprises de France (MEDEF, French



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

EXHIBIT 54.4 WORLD BANK GOVERNANCE RANKINGS: CONTROL OF CORRUPTION FOR FRANCE AND MAJOR GDP NATIONS

Business Confederation) and the Association Française des Entreprises Privées (AFEP). Unlike most reform efforts, this was not prompted by scandals; it reflected efforts to meet growing stockholder expectations. The process began with the Vienot and Bouton reports.

MEDEF and AFEP consolidated their recommendations in 2003 to make the French response complementary to those of the European Commission. Institutional investors (AFG) issued corporate governance guidelines in 2001 and 2004. The general consensus of these recommendations can be summarized:

Board Structures and Committees. After much debate it was decided to leave companies free to choose between two options:

1. A one-tier structure with a board of directors with a *président directeur général* and with a chairman and *directeur général*—chief executive officer, or CEO
2. A two-tier structure

Limitation of the Number of Offices. A director is limited from holding more than four other directorships not affiliated with his/her company.

Conflicts of Interests. Agreements made between the company and its directors must be submitted for board approval supervisory board approval, followed by a vote at the general shareholder meeting.

Board Evaluation Procedures. Boards are to meet to assess their ability to respond to shareholders expectations, by reviewing organization, and membership.

Role of Committees. Guidelines call for boards to create the appropriate committees to perform the following tasks:

- Review accounts
- Monitor internal auditing
- Select statutory auditors
- Oversee compensation and stock option policies
- Oversee appointments of directors

The consolidated code published in 2003 by MEDEF and AFEP clarifies the composition and role of the accounts, compensation, and appointment committees. Such committees have no decision-making power, such power being left to the board, and it has not been found advisable to give such committees any autonomy.

Nonexecutive Director Roles and Independence. The guidelines do not define the position nonexecutive directors nor do they mandate a proportion of nonexecutive directors. The consolidated code clearly defines the independence of directors "a director is independent when he or she has no relationship of any kind whatsoever with the corporation, its group, or the management of either that is such as to color his or her judgment."[9] The code lists the criteria that are to be used for a director to qualify as a nonexecutive director and for preventing conflicts of interests:

- Cannot be an employee, or a corporate officer of the company, its parent, or one that it has merged with over the prior five years
- Cannot to be a corporate officer of another company in which the company holds a direct or indirect directorship
- Cannot to be a customer, significant supplier, investment banker, or commercial banker of the company
- Cannot have close family ties to a corporate officer
- Cannot have audited the corporation over the prior five years
- Cannot have held a directorship for the corporation over the prior 12 years[10]

Financial Responsibility. In the event of insolvency or bankruptcy, the Consolidated Code holds directors civilly liable for violating civil or criminal laws and regulations, as well as violating the company's own rules of conduct.

Directors are also subject to administrative fines for violating disclosure regulations. These rules do not approach the United States standards that impose very harsh criminal penalties, but should act as a deterrent. With a few notorious exceptions, the loss of reputation and status is adequate to keep directors in line.

Role of Auditors. The rotation of auditors is required every six years. Their independence is also mandated by prohibiting them from holding any interest in the companies they audit. Audit firms are not allowed to offer other services to their audit clients, avoiding the types of conflicts of interests (Enron and Arthur Andersen) that lead to a breakdown in objectivity and honesty.[11]

Corporate Governance Disclosure. Board chairs are required to include in their annual reports the procedures used to prepare and organize the board's work, as well as the company's internal control procedures. (Unlike the U.S. and UK, France has not embraced the Committee of Sponsoring Organizations (COSO) framework for risk and internal controls management. Considering the limitations of COSO outlined in various chapters of this text, the French decision was a wise one. COSO I and II lack a means to quantify and measure risk. This has led to a boil-the-ocean process in the United States that has placed undue burdens on organizations with little benefit to show for their efforts.)

54.4 LOI DE SÉCURITÉ FINANCIÉRE (LSF) INTRODUCTION[12]

Effective in 2003, the LSF adds corporate governance disclosure and internal control requirements to issuers of securities. Corporate board chairs of public companies and supervisory boards of limited liability companies (sociétés anonymes) are required to annually report as part of their management report:

- The processes by which the board prepares and organizes its work (i.e., its corporate governance)
- The internal control procedures implemented by the company

As part of the LSF, external (statutory) auditors must submit their opinions and observations around the chair's internal controls as to their adequacy in preparing viable financial and accounting reports. The financial disclosure requirements are to be incorporated into the General Book of Rules of the Autorité des Marchés Financiers (AMF), the French securities regulator, which will also publish an annual report based on the information published in this respect.[13] Under the LSF, financial reporting will provide:

- A hardcopy version made available free of charge
- An electronic version posted on the AMF's web site
- An electronic version posted on the company's web site
- A news release to notify the public of the report's availability

The LSF follows French tradition in not dictating the form of a company's annual reports as long as they meet the reporting requirements of the AMF.[14]

Companies are required under Article 122 of the LSF to simultaneously publish equivalent information in the French market, that may be required under provisions of the UK's Combined Code or under the U.S.'s Sarbanes-Oxley Act. The LSF and AMF do urge companies to describe their corporate governance rules in a transparent manner and describe how these recommendations were implemented. If a company takes a different reporting path, it must explain why it has chosen for a different set of standards or type of organization.

Statuary auditors are required to report problems to corporate bodies such major deficiencies and material weaknesses in internal control procedures. In turn, corporate boards are required to report auditor findings of such problems to the public, especially if they would impact the company's share price.

54.5 LSF AND AMF PUBLICATION REQUIREMENTS SUMMARY

The disclosure and publication requirements for companies making public offerings of securities will be incorporated into the General Book of Rules of the Autorité des Marchés Financiers (AMF), the French securities regulator, which will also publish an annual report based on the information published in this respect.

Pursuant to Article L.621-1 of the French Monetary and Financial Code, the AMF clarified its expectations concerning the information to be disclosed by the issuers referred to in Article 122 of the LSF.6:

- Issuers publishing in a foreign market such as the U.S. (Sarbanes-Oxley) or UK (Combined Code) are required simultaneously to publish equivalent information in the French market.
- Registration documents must include information about corporate governance, about the company's internal control procedures and the restrictions, if any, on the powers of the chief executive.
- The documents must also include the special report of the statutory auditors, referred to in Article 120 of the LSF.

54.6 INTERNAL CONTROLS—AFEP AND MEDEF RECOMMENDATIONS

The AMF recommends that issuers refer to the joint reports of the French Association of Private Companies (AFEP) and the French Employers' Federation (MEDEF), published in October 2003, for guidance on attesting to internal controls.

- The AMF wants this approach to be part of a dynamic process culminating eventually in each issuer's publishing an assessment as to the adequacy and effectiveness of its internal control systems.
- Internal control reports should describe the due diligence underlying the analysis presented by the chairman, such as interviews with senior management, discussions at the board of directors' level, and meetings with the statutory auditors and the audit committee, where applicable.

- The AMF also reminds auditors that, pursuant to their duty to report problems encountered in the course of their engagement, they must report any such major deficiency in internal control procedures to the corporate bodies. Accordingly, where the chair is informed of such major deficiency by the auditors, he/she must mention it in his/her own report.
- Furthermore, the regulations require companies immediately to make public any information which, if revealed, would have a significant impact on their share price, or any material change in information that has already been published.
- This would be the case, in particular, for a significant weakness or deficiency in the internal control systems, identified in the course of the assessment process or the diligence performed in connection with the report.

54.7 WHISTLE-BLOWER VERSUS PRIVACY PROTECTION

The Commission Nationale de l'Informatique et des Libertes (CNIL) has made available online a single authorization for whistle-blower systems that comply with its guidelines and support U.S. Sarbanes-Oxley (SOX) requirements. In November 2005, the CNIL issued guidelines to enable U.S. companies to comply with the SOX whistle-blower provisions without violating French law.

The guidelines require companies to get approval of their whistle-blower systems from the CNIL. The CNIL's process is eloquent and much like the U.S. Safe Harbor enrollment process. All the work by the company is behind the scenes and the certification is a Web-based click-through. To get approval of whistle-blower systems, companies will fill out the online authorization form and submit it to the CNIL. The CNIL will issue a receipt by mail confirming the information.

The scope of the whistle-blower scheme must be limited to financial, accounting, banking, fraud, bribery, and SOX-related matters. There are issues and restrictions related to the categories of data collected, who receives the data, the duration that data can be stored, and required security measures, and transfer precautions for data that is going to be sent from France to the United States.

Companies that want to implement whistle-blower systems that go beyond what the guideline document describes must file a regular request for authorization.

The process, which can also be completed online, takes longer and requires more information and documentation than the simple authorization. The CNIL authorizations process is designed to assure that:

- A company's whistle-blowing policy is in place that complies with the guidelines.
- The company's whistle-blowing policy is communicated to its employees.
- Works councils or union representatives are involved where appropriate.
- Companies comply with applicable data protection law.

- There are in place third-party contracts for companies hosting the whistle-blowing hotline.
- Suitable cross-border data-flow agreements are in place to support the movement of personal data into and out of Europe.[15]

54.8 CONCLUSION

France has made significant progress in corporate governance and done so in a more sensible manner than the scandal-driven reforms of the United States. There are areas that need improvement and many of these are common for most other EU nations. These recommendations would propel France ahead of its neighbors and make it a global role model:

- Achieving a 100 percent independence of audit committees
- Achieving a 100 percent independence of remuneration/compensation committees
- Achieving a 100 percent independence of board of director chairs
- Increasing board member compensation to well above EU averages
- Improving board diversification by substantially increasing the participation of women
- Increasing the rights of minority shareholders

Notes

1. Wikipedia, Yahoo! Finance, and Euronext web sites.
2. Michel Goyer, "The Transformation of Corporate Governance in France," Brookings Institution, January 2003.
3. Ibid.
4. World Bank, "Comparison within One Country for All Six Governance Indicators," http://info.worldbank.org/governance/kkz2005/sc_country.asp.
5. Heidrick & Struggles, "Corporate Governance in Europe: What's the Outlook? 2005 Study," France, 20–21, www.heidrick.com.
6. Ibid.
7. Ibid.
8. Ibid.
9. Joëlle Simon, "Corporate Governance in France: Company Law and Corporate Governance Codes," January 23, 2004.
10. Ibid.
11. Ibid.
12. Loi de Sécurité Financière, dated 1 August 2003, published in the Official Journal of the French Republic.
13. Article L.621-1 of the French Monetary and Financial Code, in which the AMF clarifies information to be disclosed by the issuers referred to in Article 122 of the LSF.6.
14. Instruction issued in December 2001 pursuant to COB regulation 98-01.
15. Melissa Klein Aguilar, "France OKs Online Approval of Whistleblower Plans," *Compliance Week*, January 17, 2006.

CHAPTER 55

GLOBAL COMPLIANCE: GERMANY

Georg Stadtmann
Markus F. Wissmann

In this article we summarize the most recent developments in compliance in Germany. We show that Germany has developed over time from a stakeholder-oriented corporate governance system toward a shareholder-oriented system. Most recent developments in accounting and auditing are driven by European directives and regulations.

In the case study part we show that compliance/noncompliance with the German Code of Corporate Governance with regard to the disclosure of executive compensation led to the inception of a law enforcing disclosure. In an empirical analysis we show that the compensation between members of the management board and others differs greatly among companies.

55.1 REGULATORY COMPLIANCE OVERVIEW

(a) POLITICAL AND CULTURAL ENVIRONMENT. Corporate governance systems may be differentiated between shareholder- and stakeholder-oriented systems. Shareholder-oriented systems such as the U.S. system focus on modeling the

principal-agent relationship of shareholders and top management.[1] Stakeholder-oriented systems also take the interests of employees, vendors, debt financers, and other stakeholders into account.[2] Corporate governance systems are not static but develop over time and implement new elements. The development of corporate governance systems is determined by socioeconomic factors such as capital markets, legal systems, banking systems, and the ownership structure of listed corporations.[3] The development of governance systems is also attributable to the system competition of the prototypes of the above-characterized systems, namely the U.S. and the continental European systems. Governance systems may therefore change their future paths.[4]

Germany had in the past a stakeholder-oriented system. The lessons learned from the World War II led to the co-determination in the supervisory board. Co-determination refers here to the supervisory board of companies. The laws defining co-determination in Germany are:

- Coal, Iron, and Steel Industry Co-Determination Act (Montanmitbestimmungsgesetz from 1951) refers to the coal, iron, and steel industry only. This leads to parity co-determination in the supervisory board.
- Works Constitution Act (Betriebsverfassungsgesetz from 1952) refers to companies in other industries with between 501 and 1,999 employees. Employees may occupy one-third of the seats on the supervisory board.
- Co-Determination Act (Mitbestimmungsgesetz from 1976) refers to all forms of companies with more than 2,000 employees. The Co-Determination Act establishes an equal number of representatives from the shareholders' side and the employees' side. In case of a tie vote in the supervisory board, the chairperson has two votes on the second ballot. Since the chairperson is nominated by the shareholders, this side is always overrepresented by one vote.

The development path of the German corporate governance system has partly changed toward shareholder orientation starting with the inception of the KonTraG in 1998. Nevertheless, due to the Co-Determination Act, German companies still have to take the interests of the workers into account. The legal foundations for listed companies are outlined in the joint stock companies code (Atkiengesetz, AktG), which sets up a two-tier board system with a management board and a supervisory board. The German market for corporate control of public companies is considered to be underdeveloped relative to other industrialized countries, as relatively few banks exercise control of the supervisory board through the pooling of shareholders' voting rights and the low market capitalization of most companies. As a reaction to corporate scandals around 1998, the focus of the German corporate governance legislation has been shifted to shareholders, whereby the consistency of the German corporate governance system, as defined earlier, has been maintained.[5]

The majority of public limited companies are organized as limited companies (Gesellschaft mit beschränkter Haftung, GmbH),[6] but compliance is primarily

an issue for listed companies, which are publicly traded. In our contribution we focus on listed companies (Aktiengesellschaften, AG).

(b) LEGAL ENVIRONMENT

(i) Law for Joint Stock Companies. The German legal system for listed companies is a two-tier system with a managing board and a supervisory board. The supervisory board appoints the members of the managing board with at least a majority of two-thirds for a period not exceeding five years.

Managing the companies business is the responsibility of the managing board. The members of the managing board jointly manage the company. However, the managing board may modify this principle by a resolution that allows each member to manage his/her own area. The members of the managing board have to apply due diligence in their acting (§ 93 I 1 AktG) and have to obey the respective laws. The managing board also has to inform the supervisory board, who in turn uses this information to monitor the managing board. The German codex on corporate governance chapter 3.4 demands that the supervisory board shall give concrete guidance to the managing board as to which information and reports are required. The shareholders' meeting is called by the managing board, while the agenda for the shareholders' meeting and recommendations regarding the voting of the shareholders are given by the managing board. According to § 15 WpHG (Securities Trading Act), all share-price relevant data has to be published by the managing board immediately. All shareholders should be treated equally (§ 53 a AktG). According to chapter 6.3 DCGK, all data made available to analysts shall be made available to the shareholders. According to § 119 II AktG, upon initiative by the managing board the shareholders' meeting may decide on a certain topic.

The supervisory board has to monitor the managing board and appoints and dismisses the members of the managing board. The supervisory board therefore may influence the company's business by appointing certain persons to the managing board.[7] For certain transactions the permission of the supervisory board may be needed (§ 111 IV 2 AktG). The Transparenz- und Publizitätsgesetz (TransPuG) demands a catalog of transactions for which approval by the supervisory board is required. According to chapter 5.1.1 DCGK, the supervisory board has to consult and support the managing board continuously. This is a development to a more active role of the supervisory board compared to the past in § 111 I AktG. § 95 AktG sets the maximum number of members of the Co-Determination Act.[8] The supervisory board organizes itself. Certain expert committees may be considered useful in applying due diligence in the supervisory board.

The shareholders' meeting, which represents the shareholders, appoints the supervisory board, which in turn has to monitor the managing board.

(ii) Securities Laws. The Securities Trading Act (Wertpapierhandelsgesetz) regulates insider surveillance, the monitoring of compliance with the prohibitions

against stock exchange and market price manipulation, the notification and disclosure requirements in the event of changes in the percentage of voting rights in listed companies, the rules of conduct for investment services enterprises, and aspects regarding financial analyses and limitation of compensation claim rights, the liability for incorrect or omitted capital market information, financial future transactions, arbitration agreements, foreign organized markets, the monitoring of company financial statements, the regulations regarding criminal penalties, and administrative fines. The Securities Trading Act applies to the provision of investment services and noncore investment services, to on- and off-exchange trading in financial instruments, to the conclusion of financial future transactions, to financial analyses, and to changes in the percentage of voting rights held by shareholders of listed companies. Securities within the meaning of the Act, whether or not represented by a certificate, are shares, certificates representing shares, bonds, profit-participation certificates, warrants, and other securities that are comparable to shares or bonds (Section 2.1).

With regard to compliance of particular interest is insider surveillance. Under the Act it is prohibited to make use of inside information in order to acquire or dispose of insider securities for one's own account or for the account of or on behalf of a third party; to disclose or make available inside information to a third party without the authority to do so; or to recommend, on the basis of inside information, that a third party acquire or dispose of insider securities, or to otherwise induce a third party to do so. Immediate public disclosure is required from an issuer of financial instruments that are admitted to trading on an organized market within Germany, or for which it has applied for such admission, regarding all inside information that directly concerns that issuer. Persons discharging managerial responsibilities within an issuer of shares are obliged to notify the issuer and the Supervisory Authority (Bafin) of their own transactions in shares of the issuer or financial instruments based in them, in particular derivatives, within five business days. This also applies to other parties closely associated with such persons.

On July 1, 2005, the new Securities Prospectus Act (Wertpapierprospektgesetz, WpPG) came into effect. This law implements the EU Prospectus Directive (2003/71EC). Under the Act issuers whose home member state is Germany and whose securities are traded on a regulated market provide annually a document that contains or refers to all information they have published or made available to the public over the preceding 12 months. This document covers ad hoc disclosure, disclosures about directors' dealings, disclosures requirements in the event of changes in the percentage of voting rights in the listed companies, notice of stockholders' meetings, interim reports, notes of dividend payments, notice of issuance of new shares, annual financial statements and management report, and notices required under foreign law.[9]

Also under the new Securities Prospectus Act, companies that implement stock option programs may have to publish a prospectus if the relevant program provides for a "public offer of securities." No obligation to publish a prospectus exists when the shares are already admitted to trading on an organized market or by an affiliated undertaking with the meaning of the AktG. This is in particular relevant for U.S. or Asian groups that offer shares of stock in listed holding companies to the employees of their German subsidiaries, which are traded in the market segment open market in Germany. Also trading in the home market is not sufficient to circumvent the prospectus requirements. Only markets within the European economic area are recognized as organized markets. Fines for infringement of the WpPG are up to 500,000 euros.[10]

(c) ACCOUNTING AND FINANCE ENVIRONMENT. The principles of accounting are codified in the German Commercial Law and have historically been dominated by the prudence principle. With the globalization of capital markets the most recent development in accounting and finance is driven by the developments on the European level. Germany transformed the Fair Value Directive, the IAS regulation, and the imperative regulations modernization directive (directive 2003/51/EC) into national law. Therefore, all European parent companies have to apply International Financial Reporting Standards (IFRS) on their consolidated financial statements for reporting periods beginning on or after January 1, 2005.

The German Accounting Standards Committee (GASC) develops recommendations on the principles applied on consolidated financial statements, consults the Ministry of Justice, represents the Federal Republic of Germany in international standard setting bodies, and works together with the IASB and other standard setters. The standards developed by the GASC established the DSR (Deutscher Standadisierungsrat), which develops recommendations for the application of the principles of consolidated financial statements, which, once approved by the Ministry of Justice, are transformed into German Accounting Standards (Deutsche Rechnungslegungstandards, DRS). The DRS complement the German commercial law but are not allowed to contradict the commercial law.[11]

With the enactment of KonTraG in 1998 (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), there has been a shift in the German corporate governance system toward greater responsibility of management and the supervisory board. First, it attempts to improve risk management practice and requires the introduction of a monitoring system that identifies risks that might affect the going concern of joint stock companies. The supervisory board has to verify the effective use of this system by management, which has to report any risk identified by the monitoring system to the supervisory board.[12] Second, as with

SOX, the monitoring system is subject to a regular external audit. With KonTraG the legislature focused on transparency and control. This led to a paradigm shift in the German corporate governance system from a stakeholder-oriented system toward a shareholder-oriented system.[13]

An important event in the evolution of German corporate governance toward more transparency is the implementation of the German Corporate Governance Code. The TranPuG implemented § 155 AktG which demands a yearly report on compliance with the German Codex on Corporate Governance. Within the codex recommendations and suggestions are outlined. The corporate governance codex itself follows the principle of comply or explain, which means that deviations from recommendations within the corporate governance codex have to be named, whereas deviations from suggestions need not to be named. The intention is to single out companies that decide not to comply with its principles and rely on public pressure rather than formal sanctions to improve German corporate governance.

The supervisory board (Aufsichtsrat) has to be informed by the managing board of directors (Vorstand) of deviations from targets reported earlier. Furthermore, the supervisory board has to meet twice a year. The supervisory board has to discuss the consolidated financial statements after a presentation given by the external auditors on significant findings during the audit and has to approve the consolidated financial statements. The supervisory board has to issue a report on the approval of the consolidated financial statements. The German commercial law was changed in the respect that a cash flow statement and a report on equity movements are now part of the consolidated financial statements of all listed companies. Tax-driven valuations are no longer permissible in the consolidated financial statements. The TransPuG made the audit of the monitoring system introduced by the KonTraG mandatory for all companies listed on a stock exchange and not just for listed companies.[14]

The BilReG (Bilanzrechtsreformgesetz) increased auditor independence and made IFRS/IAS mandatory for listed companies. Further, companies that are traded in a regulated market have to disclose the fees for their auditors.[15] Fees have to be reported for audit services, other assurance and attestation services, tax services, and other services. The intention of the legislator is to increase transparency with regards to potential conflict of interest of the external auditors. Derivative financial instruments such as options, futures, forwards, and swaps and their fair values have to be disclosed in the notes to the financial statements.[16] The BilReG also changed the focus of the management report from purely focusing on risks to also focusing now on chances inherent in the company's environment. The legislator wanted to increase the decision usefulness of the management report and to enable investors to understand the business and not just the financials. DRS 15 also introduced a structure for the management report of consolidated financial statements, which will lead to more uniform and comparable analysis; the BilReG makes explicit reference to DRS 15, which has to be applied for

reporting periods beginning after December 31, 2004. DRS 15 outlines basic principles for the management report:

- Completeness (all relevant information has to be included)
- Reliability (information in the management report has to be separated from the financial statements and other company information)
- The view of the managing board
- Concentration on sustainable values (all known events, decisions, and factors have to be named and explained that are likely to affect the future value of the company, according to management)[17]

The management report is included in the enforcement procedures of DPR and the BAFin.[18] The BilReG complements the KonTraG, whose primary focus was on risk.

The VorStOG mandates for reporting periods beginning after December 31, 2005, that the compensation for the members of the managing board is disclosed on an individual base. The compensation has to be separated into performance- and nonperformance-based components. The VorStOG is a reaction from the legislature, which transformed DCGK 4.2.4 into law since according to the legislature only a few companies complied with DCGK 4.2.4 and disclosed the compensation of the members of their managing boards. However, the general assembly may opt out from the provisions of the VorstOG by voting with a minimum majority of 75 percent.

(d) AUDITING ENVIRONMENT. Germany has anticipated the Eighth EU directive from October 11, 2005 (directive on statutory audits of annual accounts and consolidated accounts), and established the Auditor Oversight Commission (Abschlussprüferaufsichtkommission, APAK). The APAK is responsible for public oversight on the German Chamber of Public Accountants (Wirtschaft sprüferkammer, WPK) from January 1, 2005, on. The APAK is a body sui generis formed by individuals without legal capacities and supervised by the Federal Ministry of Economics and Labor. It acts independently and unbound by any instructions.[19] Oversight is carried out with respect to individuals who are entitled to carry out statutory audits or who do so de facto without being entitled. According to the Auditor Oversight Commission work plan, the following areas shall be covered:

- Examination and aptitude tests for foreign auditors
- Licensing of individuals and firms, revocation of licenses, and registration
- Disciplinary oversight
- Quality assurance
- Adoption of professional rules

Particular emphasis will be on disciplinary oversight and quality assurance.[20] Within the oversight framework, the APAK assesses whether the

WPK fulfills its obligations as established by the Public Accountants Act in a suitable, adequate, and proportional manner.[21]

The German Chamber of Public Accountants assists its members in all issues related to the professional duties. It maintains a professional register that contains professional data on members. It assists courts, public authorities, and interested third parties with relevant technical knowledge and experience upon request. The chamber also mediates where there is dispute or disagreement between members and their clients. Together with the chief prosecutor's office, the chamber is responsible for oversight of the profession. It is responsible for the approval and registration of public accountants and coordinates and administers the external quality assurance system together with APAK and administers the professional examination for public accountants.[22]

On December 21, 2004, the BilKoG (Bilanzkontrollgesetz) was enacted and a two-phased enforcement procedure was established.

In contrast to enforcement bodies in other countries, the Financial Reporting Enforcement Panel (FREP) is a private body that acts in accordance with the Ministries of Finance and Justice, whereas the BaFin (Federal Financial Supervision Authority) is a federal body.

The FREP proves whether the last financial statements and the management report or the last consolidated financial statements and management report of listed companies are compliant with the applicable generally accepted accounting principles (GAAP). The enforcement procedure phase occurs either when there is a concrete occasion, upon request of the BaFin, or on a sample basis.[23] The FREP cooperates on a national basis with WPK and APAK. Violations that come to the attention of the WPK are communicated to the FREP.[24] The FREP cooperates with companies it audits, whereas the BaFin enforces its audit with public measures in case the company does not cooperate with the FREP. BaFin also takes over from FREP if the audited company disagrees with the conclusion of the FREP or if there is considerable doubt with regard to the conclusion of the audit of the FREP.[25]

With the enactment of the Eighth Directive of the European Parliament and of the Council on May 17, 2006, considerable changes within the next two years will be required. Some commentators compare the Eighth Directive to the impact of the SOX legislation in the United States.[26] As with SOX, there is high emphasis on professional ethics (article 21), the reinforcement of auditor independence and objectivity (article 22), determination of audit fees (article 25), quality assurance (article 29), investigation and penalties (article 30), auditors' liability (article 31), and public oversight (articles 32–34).

(e) PEOPLE AND PROCESS. The recent developments in compliance in Germany have been initiated by a number of financial scandals like Holzmann or Flowtex. Germany focused in its legal initiatives described earlier on the optimization of internal and external corporate governance structures. This has

been supported by the Cromme Commission, which is now the established standard setter for corporate governance.[27] In 2001 the government commission on corporate governance had been established, led by Professor Theodor Baums. Subsequently, the Commission on German Corporate Governance Code—led by Gerhard Cromme—was called up, which developed the German Corporate Governance Code. The focus was on overcoming criticism by participants of the international markets about the German corporate governance system. The main points of criticism had to do with transparency, independence of the supervisory board, independence of the external auditors, and neglect of shareholders' interests.

Exhibit 55.1 provides an overview of the recent process in compliance in Germany.

Law	Year	Focus Points
KonTraG, KapAEG	1998	Risk management, increasing independence of supervisory board and external auditors
Report of the government commission on corporate governance	2001	150 recommendations for the government
German Code on Corporate Governance	2002	Standards on good governance
TransPuG	2002	Increase information basis of supervisory board
Fourth financial market support law	2002	Liability of issuers for flawed ad hoc communication
Ten-point program on German government	2003	Increase investors' confidence
Amendment to German Code on Corporate Governance	2003	Recommendations on remuneration of managing and supervisory board
AnSVG	2004	Increased ad hoc publicity and prevention of insider trading
BilReG	2004	International Accounting Standards, independence of external auditor
BilKoG	2004	Enforcement on the correctness of external financial reporting
APAG	2004	Supervision of public accountants
Amendment DCGK	2005	Increase independence of members of supervisory board
VorstOG	2005	Individual disclosure on remuneration of members of managing board
UMAG	2005	Facilitation of legal actions by shareholders
KapMUG	2005	Bundling of capital market legal actions in model cases

EXHIBIT 55.1 OVERVIEW OF COMPLIANCE IN GERMANY

55.2 CASE STUDY: TRANSPARENCY OF EXECUTIVE COMPENSATION IN GERMANY

(a) INTRODUCTION AND THEORETICAL BACKGROUND. The transparency of the compensation of the members of the management board has become a central element of the German corporate governance system. The German Corporate Governance Code (GCGC) was introduced on February 26, 2002.[28] In the first version of the Code, the transparency of the individual compensation of the members of the management board was formulated as a suggestion. Since the revision in May 2003, this passage was upgraded to a recommendation. As a consequence, companies were obliged to disclose their deviations from all recommendations (comply or explain). Due to the fact that only a minority of all publicly listed companies followed the recommendation of the GCGC, the Ministry of Justice introduced a law on August 3, 2005, that will force publicly listed companies to report the compensation of members of the management board on an individual basis. This new regulation will be applied for those consolidated financial statements for business years that start after December 31, 2005.

Traditional principal-agent (PA) models assume that both principals and agents act fully rationally and only in their own interests. Furthermore, both parties know about each other that both parties act rational and are also aware of their conflicts of interest. The technical solution of a traditional PA model foresees setting up a contract where the fixed part of the compensation is negative while the agent is allowed to receive 100 percent of the company's profits as the variable part of the compensation. The participation constraint assures that overall compensation for the agent is marginally positive. This secures agents' willingness to sign the contract (participation constraint). However, traditional PA models fail to predict how transparency of co-workers' compensation will impact the effort. Since every agent acts fully rationally and concentrates only on his/her own amount as well as the structure of compensation, there is no difference between whether or not an agent knows about co-worker's wage. Transparency or intra-transparency does not matter.

In some recent contributions to the literature, it is assumed that fairness aspects also matter.[29] Charness and Kuhn (2004) assume in a model with one principal and two agents where the agents compare their compensation levels in a case in which this information is transparent. Each agent compares reciprocally whether he/she is treated fairly or unfairly. The outcome of this comparison is reflected in the agents' effort function in the following way:

$$A_i = aw_i + b(w_i : w_j)$$

Therefore, the effort level (A) of agent i is a function of his/her own wage level as well as of the wage differential. In the case that the agent's j wage is larger than agent's i wage level ($w_j > w_i$), agent i will withhold effort compared

to a situation without any wage differentiation. Charness and Kuhn (2004) show that transparency will decrease the degree of wage differentiation. Furthermore, it can be shown that the sum of compensation for both agents can be higher in a transparent scenario compared to an intra-transparent scenario. The higher wage bill implies a cost increase, so that the profit of the principal decreases.

Charness and Kuhn (2004) take an internal company perspective. In contrast to this, Ezzamel and Watson (1998) take an external view when analyzing the effects of transparency in the market for British executives. They analyze how transparency influences wage comparisons between different companies.

They argue that transparency allows one to compute an average wage level for executives. Compensation committees will use this information in their decisions. This is not only valid for the British system but also in line with the German Corporate Governance Code: As is stated in 4.2.2 GCGC, the supervisory board should, among other things, consider "the performance and outlook of the enterprise taking into account its peer companies."

Ezzamel and Watson (1998) argue that it is more likely that underpaid executives' wages will be increased than overpaid executives' wages adjusted downward. Due to this asymmetry, the average wage level will increase, leading to further adjustments over time. They call this process the bidding-up phenomenon.[30]

(b) DESCRIPTIVE STATISTICS. Until 2004, 18 of the DAX-30 companies disclosed their executive compensation on an individual basis. For the business year 2004 it was the first time that the majority of the DAX-30 companies disclosed their executive compensation on an individual basis.

In Exhibit 55.2 we compare the cash compensation of the other management board members with the compensation of the CEOs of two companies. We can identify two extremes:

Cash Compensation of Management Board of TUI AG in 2004

	Fixed Compensation	Variable Compensation	Total Compensation	Total Compensation in % of CEO
Dr. Michael Frenzel (CEO)	1,405	1,101	2,506	100%
Sebastian Ebel	425	482	907	36%
Dr. Peter Engelen	412	482	894	36%
Rainer Feuerhake	785	826	1,611	64%
Total	3,027	2,891	5,918	

EXHIBIT 55.2 DIFFERENTIATION OF EXECUTIVE COMPENSATION

Cash Compensation of Management Board of Scherring AG in 2004				
	Fixed Compensation	Variable Compensation	Total Compensation	Total Compensation in % of CEO
Dr. Hubertus Erlen (CEO)	720	1,668	2,388	100%
Dr. Katrin Dorrepaal	180	415	595	25%
Dr. Ulrich Köstlin	540	1,246	1,786	75%
Lutz Lingnau	540	1,246	1,786	75%
Marc Rubin	540	1,246	1,786	75%
Dr. Jörg Spiekerkötter	540	1,246	1,786	75%
Prof. Dr. G. Stock	540	1,246	1,786	75%
Total	3,600	1,246	11,913	

Source: Own calculations/Annual Reports of 2004.

EXHIBIT 55.2 (*continued*) DIFFERENTIATION OF EXECUTIVE COMPENSATION

On the one hand, the compensation of the TUI AG executives has the higher differentiation: Two members of the board earn only 36 percent of the CEO's compensation while one board member earns 64 percent of the CEO's pay.

On the other hand, Schering AG compensates its executive board members with 75 percent of the CEO's pay. Dr. Katrin Dorrepaal, who joined the board on September 1, 2004, received only 25 percent, but this was in consideration of the short time she had served in the board.

Hence, Schering AG does not differentiate the compensation among its non-CEO board members. This compensation scheme is not in line with the German company act law (§ 87 Abs. 1 AktG as well as 4.2.2 GCGC), which says that the individual compensation should be linked to the individual tasks and the personal performance of a board member.

55.3 CONCLUSION

Due to the theoretical argument given before, we expect changes in the compensation structure as well as level of compensation in the near future.

The empirical analysis shows that the variation of compensation between members of the management board differs extremely between companies. As a consequence, empirical studies that used a static formula to extract, for example, CEO compensation from total board compensation via a static formula may be unreliable.

In the future, researchers will have access to a new data set to analyze all aspects of executive compensation in a non-Anglo-Saxon setting.

Notes

1. See Werder (2003, 7).
2. See Werder (2003, 8).
3. See Böcking (2003, 253).
4. See Witt (2003, 122).
5. See Schmidt and Spindler (2000) with regard to path dependency of corporate governance systems. Schmidt and Weiß (2003) point out that KonTraG has contributed to a paradigm shift from insider to outsider control. See also Böcking (2003).
6. See Witt (2003, 78).
7. See Oetker (2003, 263).
8. See Oetker (2003, 264–267).
9. See Cleary Gottlieb (2006, 1–6).
10. See Nordhues (2006, 1).
11. See Baetge and Hagemeister (2003, 797–799).
12. This can be derived from § 111 I AktG; see Gruson and Kubicek (2003, 395).
13. See Seibert (2003, 243).
14. See Pfitzer et al. (2006, 89–90).
15. Note that small companies according to § 267 (3) HGB are exempt.
16. See Pfitzer et al. (2006, 97).
17. See Pfitzer et al. (2006, 113–114).
18. See Böcking (2006, 3).
19. See APAK (2005a, 1).
20. See APAK (2005b, 1).
21. See APAK (2005a, 1).
22. See WPK (2006).
23. See DPR (2005, 2).
24. See DPR (2005, 7).
25. See Pfitzer et al. (2006, 151).
26. See Pfitzer et al. (2006, 285–297).
27. See PWC/BDI (2005, 14).
28. Information on the composition and compensation of executives can be found in part 4.2, GCGC.
29. See Güth et al. (2002).
30. Some authors use the label *ratcheting effect* for this phenomenon. For example, the Combined Code contains in Section B.1.2 the following recommendation with respect to the remuneration policy: Remuneration committees should judge where to position their company relative to other companies. They should be aware what comparable companies are paying and should take account of relative performance. But they should use such comparisons with caution, in view of the risk that they can result in an upward ratchet of remuneration levels with no corresponding improvement in performance.

References

APAK—Abschlussprüferaufsichtskommission/Auditor Oversight Commission. 2005a. Rules of procedure for the oversight on auditors in Germany. www.apak-aoc.de.

APAK—Abschlussprüferaufsichtskommission/Auditor Oversight Commission. 2005b. Work plan for 2005 of the commission for the oversight on auditors in Germany (Auditor Oversight Commission). www.apak-aoc.de.

Baetge, Joerg, and Christina Hagemeister. 2003. Das Deutsche Rechnungslegungstandards Committee. In Dietrich Dörner et al., *Reform des Aktienrechts, der Rechnungslegung und der Prüfung*, 2nd ed., 795–820. Stuttgart, 2003.

Böcking, Hans-Joachim. 2003. Corporate Governance und Transparenz—Zur Notwendigkeit der Transparenz für eine wirksame Unternehmensüberwachung. In Axel von Werder and Harald Wiedmann, *Internationalisierung der Rechnungslegung und Corporate Governance*. Stuttgart, 2003.

Böcking, Hans-Joachim. 2006. In: KPMG Audit Committee Institute 2006: *Audit Committee Quarterly* I/2006.

Charness, Gary, and Peter Kuhn. 2004. Do co-workers' wages matter? Theory and evidence on wage secrecy, wage compression and effort. IZA Discussion Paper 1417. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=511502.

Cleary Gottlieb Steen & Hamilton LLP. 2006. German Securities Prospectus Act. www.cgsh.com/files/tbl_s5096AlertMemoranda/FileUpload5741/367/28-2006.pdf #search='B%C3%B6rsG'.

DPR—Deutsche Prüfstelle für Rechnungslegung. 2005. Tätigkeitsbericht für den Zeitraum vom 1. Juli bis 31. Dezember 2005. www.frep.info/docs/jahresberichte/2005_tb_pruefstelle.pdf.

Ezzamel, Mahmoud, and Robert Watson. 1998. Market comparison earnings and the bidding-up of executive cash compensation: Evidence from the United Kingdom. *Academy of Management Journal* 41(2): 221–231.

Gruson, M., and M. Kubicek. 2003. Der Sarbanes-Oxley Act, Corporate Governance und das deutsche Aktienrecht (Teil II). *Die Aktiengesellschaft* 48(8): 394–406.

Güth, Werner, Manfred Königstein, Judit Kovács, and Enikõ Zala-Mezõ. 2001. Fairness within firms: The case of one principal and multiple agents. *Schmalenbach Business Review* 53(82): 101.

Nordhues, Ulrich. 2006. New German Securities Prospectus Act may jeopardize stock option programs of non-EU subsidiaries in Germany. www.mwe.com/info/news/gu0406.pdf#search='WpPG'.

Oetker, Hartmut. 2003. Aufsichtsrat/Board: Aufgaben, Besetzung; Organisation, Entscheidungsfindung und Willensbildung—Rechtlicher Rahmen. In Peter Hommelhoff et al., *Handbuch Corporate Governance*, 255–284. Stuttgart55.

Pfitzer, Norbert, Peter Oser, and Christian Orth. 2006. *Reform des Aktien-, Bilanz- und Aufsichtsrechts*, 2nd ed. Stuttgart.

PWC/BDI—PricewaterhouseCoopers/Bundesverband der Deutschen Industrie e.V. 2005. *Corporate governance in Germany*.

Schmidt, Reinhard H., and Gerald Spindler. 2000. Path dependency and corporate governance and complementarity. Johann Wolfgang Goethe Universität Frankfurt am Main, Finance and Accounting Working Paper Series 27. www.wiwi.uni-frankfurt.de/schwerpunkte/finance/wp/408.pdf.

Schmidt, Reinhard H., and Marco Weiß. 2003. Shareholder vs. Stakeholder: Ökonomische Fragestellungen. In Peter Hommelhoff et al., *Handbuch Corporate Governance*, 107–127. Stuttgart.

Seibert, Ulrich. 2003. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG): Die aktienrechtlichen Regelungen im Überblick. In Dietrich Dörner et al., *Reform des Aktienrechts, der Rechnungslegung und der Prüfung*, 2nd ed., 239–262. Stuttgart.

Werder, Axel von. 2003. Ökonomische Grundfragen der Corporate Governance. In Peter Hommelhoff et al., *Handbuch Corporate Governance*, 3–27. Suttgart.

Witt, P. 2003. *Corporate Governance-Systeme im Wettbewerb*. Wiesbaden: Gabler.

WPK—Wirtschaftsprüferkammer/Chamber of Public Accountants. 2006. Services and duties of the WPK. www.wpk.de/english/about/services.asp.

CHAPTER 56

THE CURRENT AND FUTURE STATES OF CORPORATE GOVERNANCE CULTURE AND REGULATION IN INDIA

Sanjay Anand

Corporate governance is the cornerstone of accountability for publicly traded companies. The goal of sound corporate governance practices is to ensure that the interests of the shareholders, the people who own shares in the publicly traded company, are protected. It was not until the 1990s that corporate governance was contemplated seriously. This brought in a new era of business as the cold war ended and business opened up on a global scale with the birth of the Internet and the creation of a global village. Since then, many developed countries have raised the bar on corporate governance, generally in the wake of serious scandals in which publicly traded companies have demonstrated severe ethical mismanagement of company funds.

The United States has set the standard for corporate governance with the implementation of the Sarbanes-Oxley Act in 2002. This act has set forth strict guidelines regarding the accountability and reporting of the governing body of publicly traded companies. It has also set forth strict and severe punishments for any person or enterprise that violates the law as set out by the Act. While there has been an effort to create controls on corporate governance in India, until recently they fell far short of the guidelines presented in the Sarbanes-Oxley Act and the norm of good corporate governance on the global scale.

In India, corporate governance has been hindered largely by the ethical atmosphere of publicly traded companies. In other words, there has been little or

no accountability and, until recently, there have been no restrictions on the level of independence of the board of directors. While there certainly are ethically run companies in India, N. Vittal, India's Central Vigilance Commissioner, in his paper *Issues in Corporate Governance in India* (2002), indicates there have not been strict enough penalties for those who do not follow good or decent corporate governance practices. Therefore, unless the governing body of a company is ethical, they would easily be tempted to run the company by unethical means. Either they would not be caught or the punishment would not be severe enough to deter such behavior in the future and they were well aware of this. However, as described in the case study that follows, exposure to the global marketplace fosters an increase in corporate governance standards within companies.

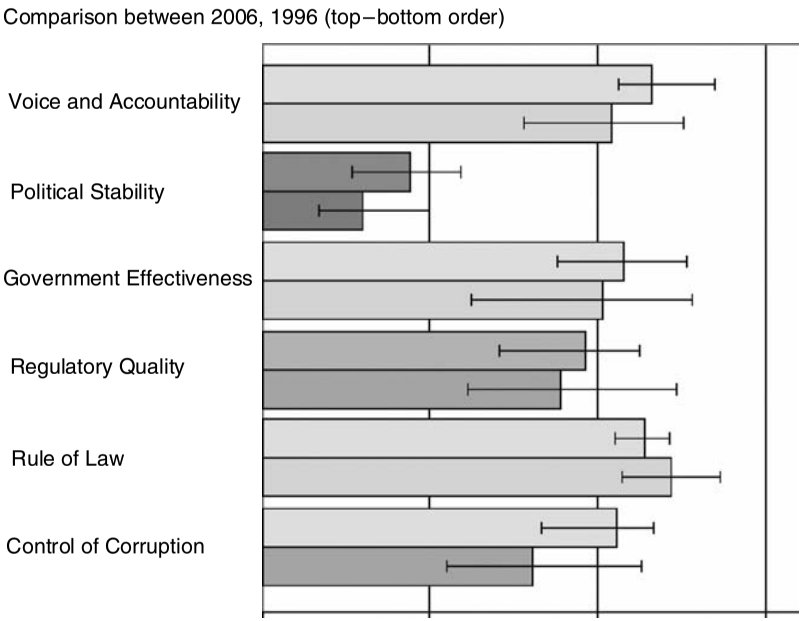
Vittal also points out that while corporate governance is centered on ethics, it is not just based on the ethics of the management team itself, but is also part of the ethical atmosphere of society. In other words, it can be quite simple for a company to defend a behavior on the basis of what the prevailing norm is, such as in the case of the Harshad Mehta scam. In this situation, management claimed that the bank receipts were handled in a manner consistent with the prevailing norm. The current social values of society can make something acceptable even when it is clearly not ethical and management must be able to withstand social pressure and the temptation to use societal norms as a way to mismanage company funds.

The World Bank is an organization committed to aiding the effort to alleviate poverty across the globe and they consider good corporate governance and anticorruption measures to be critical to meet this end. They have been monitoring corporate governance indicators of their member countries since 1998 and they have found that the state of India's corporate governance atmosphere has worsened overall between 1998 and 2004, the year that Clause 49 (see later) was amended (World Bank 2006) (See Exhibit 56.1).

The results of the World Bank research signify that in five of the six indicators of corporate governance, India performed more poorly in 2004 than in 1998. Only in the area of government effectiveness was there an improvement, taking it from the 50th percentile to the 55th percentile. There was a decrease in effectiveness of the other five indicators: voice and accountability, political stability, regulatory quality, rule of law, and control of corruption. This decrease is in relation to other countries, but the significance of the outcome of this research is that it is obvious that India has not been keeping up. This indicates that not only has India not been progressing in the area of corporate governance, the situation has been getting progressively worse relative to the global standard, and in this current global society this situation will only hinder India's economic development. It is interesting to note that, according to the same study, India is either on par with or ahead of the regional average. This does not bode well for corporate governance in the region of South Asia.

Mukherjee and Ghosh in their paper, "An Analysis of Corporate Performance and Governance in India: Study of Some Selected Industries" (2004),

Governance Indicator	Year	% Rank (0–100)	Governance Score (–2.5 to +2.5)	Std. Error	Sources
Voice & Accountability	**2006**	**58.2**	**0.35**	**0.15**	**13**
	1996	**52.2**	**0.12**	**0.24**	**5**
Political Stability	**2006**	**22.1**	**–0.84**	**0.22**	**10**
	1996	**14.9**	**–1.12**	**0.29**	**5**
Government Effectiveness	**2006**	**54**	**–0.04**	**0.16**	**13**
	1996	**50.7**	**–0.19**	**0.23**	**7**
Regulatory Quality	**2006**	**48.3**	**–0.15**	**0.18**	**11**
	1996	**44.4**	**0.02**	**0.23**	**7**
Rule of Law	**2006**	**57.1**	**0.17**	**0.13**	**17**
	1996	**61**	**0.26**	**0.19**	**9**
Control of Corruption	**2006**	**52.9**	**–0.21**	**0.13**	**15**
	1996	**40.3**	**–0.36**	**0.2**	**7**



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, "Governance Matters V: Governance Indicators for 1996–2006" (World Bank, July 2007).

EXHIBIT 56.1 WORLD BANK GOVERNANCE RANKINGS: SIX ELEMENTS FOR INDIA 2006 AND 1996 (TOP-TO-BOTTOM ORDER)

outline the major weaknesses within the corporate governance structure in India. These weaknesses are based on the level of autonomy of management that has resulted from the inability to create a thorough contract between the financer (shareholders) and management. Thus, there are three key areas in which there are issues or problems that generally arise. These are:

1. Fund allocation
2. Poorly performing managers
3. Poor project selection by management

According to Mukherjee and Ghosh, in India the main problem has stemmed from the lack of independence of the board of directors. This leads to many problems, because directors who are not independent can make choices to benefit themselves rather than the company and the shareholders' bottom line. Although there is now a requirement to ensure the independence of directors (see Clause 49, the next section), there is an inadequate supply of qualified and high caliber directors available. These directors need to be high caliber to instill confidence in the shareholders and they need to be experts in the field so that they can contribute something of worth to the company rather than simply be present to oppose management. The conclusion drawn is that corporate governance in India is still in its early stages of development, but hopefully with models like the Sarbanes-Oxley Act and the Cadbury Code of Great Britain and the creation and amendment of Clause 49, it will soon be more competitive in the global marketplace.

56.1 CLAUSE 49

Clause 49 is attached to the listing agreement that exists between a publicly traded company and any of the Indian stock exchanges. This clause has been put in place by the Securities Exchange Board of India (SEBI) to ensure proper corporate governance of Indian companies (Patel 2006). While Clause 49 was originally instituted in 2000, it was amended in 2004 to fall more in line with the Sarbanes-Oxley Act of the United States in order to enhance the corporate governance practices required by companies and to ensure scams such as the Harshad Mehta scam and the Ketan Parikh scam are not repeated.

When Clause 49 was first introduced to the publicly traded sector, the goal of the clause was to establish basic corporate governance practices throughout corporate India.

These practices included:

- The minimum number of independent directors required on the board of a company was specified.
- The establishment of an audit committee and a shareholders' grievance committee, and other critical committees were made mandatory.

- Management's Discussion and Analysis (MD&A) section, the Report on Corporate Governance in the Annual Report, and disclosures of fees paid to nonexecutive directors were made mandatory.
- A limit was placed on the number of committees on which a director could serve.

With the introduction of the Sarbanes-Oxley Act in 2002, SEBI took another look at Clause 49 and decided that it was not rigorous enough. In 2004, an amended version of Clause 49 was introduced in order to ensure that it was an effective enough control on corporate governance. With these amendments came recommendations that were mandatory and recommendations that were voluntary. The mandatory recommendations were as follows:

- *Clarifies the standards of independence for directors.* This rigorous legislation has put in place a three-year cooling-off period for any member of any advisory firm, including auditors, lawyers, consultants, and internal auditors. SEBI has also clarified that government nominees on boards should not be considered independent.
- *Clarifies and increases the responsibilities of the board of directors.* The revised clause serves to enhance the responsibilities of the board of directors. The board is now responsible for the company's compliance with all applicable laws and enhanced oversight over its subsidiaries. The board is also required to evaluate the company's risk management framework, to assess all significant transactions entered into by any subsidiary as well as appraise the minutes of all the subsidiaries' board meetings, and to sign-off on compliance with the company's code of conduct.
- *Improves the quality and quantity of disclosures.* The number and quality of disclosures required has been increased substantially. These disclosures include directors' shareholding in the company, compensation paid to nonexecutive directors, all related-party transactions, use of funds raised through public issues (in case of any use of funds for purposes other than that originally stated in the offer prospectus), an audited statement on the deviation to be included in the annual report, and any changes in accounting policies and practices.
- *Consolidates the predominance of the audit committee in all matters relating to internal controls and financial reporting.* It is now required that all changes in accounting policies are to be reviewed by the audit committee as are financial statements of subsidiary companies. The MD&A section of the annual report, which was previously only a board responsibility, now needs to be evaluated and accepted by the audit committee before going to the board.
- *Enhancing accountability of the CEO and CFO.* This amendment has been inspired by the Sarbanes-Oxley Act. It is now mandatory that the CEO and CFO certify to the board a minimum of once per year on matters relating to

the accuracy of financial reporting, evaluation of design and operation of internal controls, disclosure of any significant changes in internal controls, and disclosure of frauds. It is generally agreed upon by the majority of corporate managers and investors that these requirements are crucial in bringing Indian capital markets and governance standards up to par with respect to the rest of the world.

The voluntary recommendations strive to:

- Help companies create an atmosphere of management that provides for unqualified corporate financial statements
- Help provide training for board members
- Provide assessment of nonexecutive directors
- Provide performance reviews by a peer group that consists of the entire board of directors, not including the director being evaluated

The question remains, is Clause 49 stringent enough? The answer is yes. Clause 49 is likely to be a force for change within the corporate community. It will take time for it to be implemented within companies, especially those that have fallen far short of proper corporate governance standards, but the results will be to place India on the map as a contender in the global marketplace. The adoption of Clause 49 will lend credibility to Indian companies and help fuel a new era of business within the country.

56.2 THE PUBLIC SECTOR

Good corporate governance practices are not only relevant to private industry, but they are also critical in the public sector. Until recently, the attitude was one of, "We don't need that. It's for the other guys." In India, corporate governance on the public level has been addressed by a number of people. In a report entitled "The First Principles of Corporate Governance for Public Enterprises in India" (2001), Dr. Y. R. K. Reddy, chairman of Yaga Consulting Pvt. Ltd, suggests that, while the general corporate governance structure that has been brought forward for private companies is adequate when considering the public sector, there are some important pieces missing. Specifically, these codes tend not to address the special features of government control systems.

Three factors have influenced the level of good corporate governance in the developed world in places in which capital markets are alive. These are:

1. The shift in control when an organization's ownership is dispersed
2. The Cadbury Committee's Report
3. The anticipation that market efficiency will act as the definitive solution to corporate behavior and performance

These codes and principles are creating in developing countries an understanding of and a desire for the need for good corporate governance, especially in

countries in which capital markets are expanding rapidly. The problem lies in the fact that the key business and commercial sectors of the economies in the developing countries are not included in the corporate governance regulatory net or they have not found the principles to deliver the benefits they had expected. This is with regards to commercially oriented public organizations, which are under government control and public organizations that are incorporated because both listed and unlisted public organizations are ahead of private sector listed companies in terms of contribution to GDP, capital employed, income, employee strength, and social impact. It is also now being considered that public organizations lead the way in the arena of profitability.

The public sector in India includes any organization in which the government holds 51 percent or more of the equity. In 1996 the Standing Conference of Public Enterprises (SCOPE) in New Delhi that recognized the need to ensure that there was a corporate governance structure in place that was suitable for public institutions. It was clear that although there were admirable codes at the time, such as the Cadbury Code and the Confederation of Indian Industry Code, they were not made to address the specific maladies that existed in the corporate governance of Indian public organizations.

When considering public organizations, it is crucial to include all organizations at both the central and state level. At the state level there are organizations that undertake commercial activity such as state level public enterprises, state controlled cooperatives, organizations created by special statutes, joint ventures of state and central governments, departmental undertakings, companies promoted by developmental financial institutions of the government. While good corporate governance in the private sector will certainly help the economy of India and other developing countries, it may be even more crucial that the public sector displays proper corporate governance policies and procedures. This is due to the correlation that exists between good governance and good corporate governance as corporate governance is based on the democratic system.

What follows is a shortened version of the First Principles as laid out by Dr. Reddy in his report (Reddy 2001). Proper corporate governance on a public level entails the government follow these First Principles:

- The government should review the legal status of all organizations controlled by it so as to separate those which can carry out commercial activities as companies following the market discipline and those that will continue as a sovereign function of the government.
- The government should draw up a consensus-based comprehensive policy of privatization, of both companies and other entities, delineating those, which will continue to be state-owned, the method of disengagement, and the process of disengagement.
- The government should issue guidelines, policy, or directives indicating the contingent conditions under which a currently private sector activity will be brought under state control.

- The continued ambiguity in the set of objectives of public enterprises should be resolved by the government.
- The government should bring about greater transparency by fully accounting for subsidies and price controls imposed on public enterprises, and achieving the desired social and development objectives through governments' budgetary provisions and related mechanisms.
- The government should give up direct control over public enterprises by restructuring/rationalizing the role of departments overseeing these undertakings.
- The government must separate its ownership role and let public corporations be governed by the same structure of controls as that of any other company.
- Parliamentary/legislative assembly control over public enterprises should be limited to interaction with the body exercising the ownership rights of the government.
- The government should assess and recapitalize public enterprises to ensure that the cost of social burden on a historical basis is made good on a one-time basis after adjustment for special grants and concessions given, if any.
- Ownership rights of the government should be exercised by specialized bodies to be created for that purpose.
- The body exercising the voting rights should actively structure, create, develop, and renew the governing board, ensuring highest qualities of leadership, enterprise, integrity, and judgment.
- Governments must ensure that persons who are or were members of parliament or legislative assemblies be excluded from occupying positions of chairman or members of the governing board of a public enterprise.
- The position profile and specifications of chairman, CEO, and members of the governing boards should be approved by the governing board and shareholders in advance and through the expert advice of external bodies.
- Listed public enterprises will have to follow the mandatory requirements of the Company Law and the stock exchange regulations. All other public enterprises should follow the relevant CACG or OECD principles.
- Each public enterprise should develop a best practice manual for board processes, procedures, and formats.
- Public enterprises should ensure that individuals chosen for appointment as directors either are properly accredited, when such facility is available, or be formally trained in corporate governance practice.

(a) CASE STUDY: INFOSYS. One company in India has excelled in the area of corporate governance—Infosys. Infosys has been studied by numerous individuals

and organizations due to its commitment to sound corporate governance and its success in the area. It is often used as a case study and a model for other organizations in India and throughout the world. The software industry in India is a good platform from which to explore the state of corporate governance, as India has a reputable software industry that is recognized for its quality on a global scale. This is in contrast to many other companies within India, which are less likely to have a positive reputation worldwide (Khanna and Palepu 2001).

One of the main conclusions drawn from the Khanna and Palepu study is that the good corporate governance standards of Infosys did not result from global exposure, but rather, global exposure resulted from the adoption of good corporate governance standards as exhibited by countries around the world. Essentially, Infosys wanted to be able to compete in the global marketplace, not only in the realm of clientele, but also with regard to the talent pool that is available globally. It had motivation to be recognized and saw what was needed to achieve this goal. It has since become a force for changing the corporate governance atmosphere within India.

Why has Infosys implemented such a sound corporate governance strategy in a country that is far behind the global example? The company has this to say:

> We believe that sound corporate governance is critical to enhance and retain investor trust. Accordingly, we always seek to ensure that we attain our performance rules with integrity. Our Board exercises its fiduciary responsibilities in the widest sense of the term. Our disclosures always seek to attain the best practices in international corporate governance. We also endeavor to enhance long-term shareholder value and respect minority rights in all our business decisions.

The Infosys corporate governance system is based on a philosophy that follows the following principles:

- Satisfy the spirit of the law and not just the letter of the law.
- Corporate governance standards should go beyond the law.
- Be transparent and maintain a high degree of disclosure levels. When in doubt, disclose.
- Make a clear distinction between personal conveniences and corporate resources.
- Communicate externally, in a truthful manner, about how the company is run internally.
- Comply with the laws in all the countries in which the company operates.
- Have a simple and transparent corporate structure driven solely by business needs.
- Management is the trustee of the shareholders' capital and not the owner.

Infosys stresses that at the core of its corporate governance practice is the board, which oversees how the management serves and protects the long-term interests of all the stakeholders of the company. It states:

> We believe that an active, well-informed, and independent board is necessary to ensure the highest standards of corporate governance. Majority of the Board, 9 out of 16, are independent members. Further, we have compensation, nomination, investor grievance, and audit committees, which are comprised of independent directors.

It is clear that Infosys is the national and regional model for corporate governance and they have proven that success, especially on a global scale, comes with the integrity and clarity of sound corporate governance.

56.3 WHAT THE FUTURE HOLDS

With Clause 49, the model that Infosys provides, and world interest, India has a bright future in the area of corporate governance. The key factor in creating an atmosphere of respectable corporate governance with tight controls on accountability is time (Patel 2006). Specifically, companies will have to struggle to conform to Clause 49 in certain areas. One such area is the composition of the board of directors. Indian companies will have to scramble to ensure they have the proper composition of independent directors and that they comply with the new definitions set forth for the term independent. As mentioned earlier, the biggest stumbling block here is the lack of individuals who are qualified (properly educated and prominent in the community) to serve as directors. The board and the audit committees will also need to carefully plan their agendas to ensure compliance as there are a number of new functions that have been made their responsibility. Boards now have to identify and examine the specific regulations that exist in their region and they must ensure that their practices are in line with these laws. This will take time. The final area in which companies will struggle to comply within the allotted time frame is in the area of risk management. Companies must identify the risks and then create plans to manage those risks.

Within the public sector it is also clear that much work is needed and that it may be even more crucial to the well being of India's economy to ensure that public organizations have a sound corporate governance structure on which to operate. With the First Principles set out by Dr. Reddy (2001), this goal can be achieved.

With these tasks facing them, both private and public companies have a large job ahead of them to ensure complete compliance with the new laws regarding corporate governance. In the end, it is the desire to compete in the global marketplace that will encourage Indian companies to revamp their corporate governance policies and strive to make more ethical and moral business decisions. However, the majority of management agrees that this is not only necessary, it is wise and just to follow proper corporate governance policies.

References

Kaufmann, Daniel, Aart Kraay, and Massimo Mastruzzi. 2006. Governance matters V: Governance indicators for 1996–2005. World Bank, July, 2007.

Khanna, Tarun, and Krishna Palepu. 2001. Governance in India and around the globe. Harvard Business School Working Knowledge, December 10.

Mukherjee, Diganta, and Tejamoy Ghosh. 2004. An analysis of corporate performance and governance in India: Study of some selected industries. Indian Statistical Institute, Kolkata, India, June.

Patel, Manesh. 2006. Inside Clause 49. *Express Computer*, February 27. www .expresscomputeronline.com.

Reddy, Y. R. K. 2001. The first principles of corporate governance for public enterprises in India. *Corporate Governance Commentary*, December 11. www.corpgov.net/forums/commentary/commentary.html.

Vittal, N. 2002. Issues in corporate governance in India. Fifth JRD Tata Memorial Series.

World Bank. 2005. Six governance indicators for India. *Governance and Anti-Corruption*. http://info.worldbank.org/governance/kkz2005/sc_chart.asp.

CHAPTER 57

INDIAN CORPORATE GOVERNANCE: COMPLIANCE VERSUS VALUE ADDITION

Sanjay Anand
C. V. Baxi
C. L. Bansal

57.1 BACKGROUND

The context factors characterizing the Indian practice of corporate governance are, among others: evolving public policy on control and regulation of Indian industry; the setting up of regulatory authorities for the banking, insurance, and financial markets; establishment of Competition Commission of India (which seeks to subsume the earlier Monopolies and Restrictive Trade Practices (MRTP) and the Board of Industrial and Financial Reconstructions (BIFR) acts); specific

amendments to the Companies Act 1956 introduced in 2003; the lack of shareholder activism; significant number of closely held companies; the relative lack of single minority share ownership; relatively passive role of the institutional investors; weak law enforcement system; multiplicity of institutions involved in regulating the corporate sector and financial markets; critical issues of succession planning and the relative rise in the status and role of the nonfamily professionals in the family-owned business; the issue of viability of the decentralized stock exchange system; relatively low capitalization of the companies in India; and the need for autonomy in the boards of public enterprises.

But even with these constraints it is heartening to note that there are few examples of best practices of corporate governance in India such as Infosys, the Tata group of companies, WIPRO Technologies, ICICI Bank, HDFC Bank, and several others that have demonstrated board leadership in taking a lead in strengthening the due process of board governance.

India has nearly 7,000,000 companies that are registered with the Registrar of Companies and only about 9,500 companies that are listed on the Indian stock exchanges. The total market capitalization has been around 25 percent of gross domestic product (GDP) in the most recent years. In the most recent years the market capitalization to GDP ratio has increased significantly. A relatively higher percentage is accounted by the state-owned enterprises in the oil and natural gas sector. The legal framework governing companies consists of: the Companies Act of 1956 (with 24 amendments up to 2004), the ministry of Company Affairs, Company Law Board, the Securities and Exchange Board of India under the SEBI Act of India, the Securities and Contract (Regulation) Act of 1956, the Depositories Act of 1996, and the Sick Industrial Companies (Special Provisions) Act (SICA) of 1985, among others. More recently the two national-level rating agencies have rated the quality of corporate governance in India (Credit Rating Information Services of India Limited (CRISIL) and Investment Information and Credit Agency of India Limited (ICRA)).

The Stock Exchange Mumbai (BSE) and the National Stock Exchange (NSE) are the two major exchanges in India. The situation of command and control has constrained the growth prospects of the corporate sector. In the absence of a developed capital market the financial institutions provided long-term capital to the industry. The system of nominee directors was evolved as a strategy for monitoring the management of the companies. The nominee directors in the 1980s and 1990s could have played an active role in directing and controlling board governance content and process; however, they were not very effective in view of the relative lack of expertise required at the board level, and also they were constrained by the CEO-dominated boards in the family-owned businesses; further, there were conflicts of interests since the nominee directors had to safeguard the interests of the financial institutions as also look after the interests of the companies and the shareholders. The debt contracts as means of corporate governance were not very effective as the borrowers violated many covenants of the loan agreements, which then involved protracted litigations.

By the mid-1980s the portfolio of the sick companies increased significantly and the government under SICA 1986 introduced a quasi-judicial mechanism in the form of the BIFR for evolving appropriate measures of rehabilitation and eventual turnaround. Due to various institutional constraints and market failures, the prospects of rehabilitation have suffered adversely and considerable shareholder value has been destroyed. Protection of creditor rights became a major issue. Corporate boards in general have been dominated by the CEOs who invariably chose demographically similar directors thus creating a strong CEO/weak board situation. Also, despite opportunities, the institutional investors were unable to direct and control the management of companies. The degree of compliance of law has remained a major issue for the regulators.

57.2 COMPANIES ACT OF 1956

The Companies Act of 1956 is one of the most comprehensive and perhaps the longest legal document concerning corporations in the world. The Act is administered by the Ministry of Company Affairs of the government of India. The Act provides rules and procedures on such activities of companies as: incorporation of a company, prospectus, allotment, management, general meeting of shareholders, maintenance of account and other books, investigation, inspection, and winding up, among others. Further, such critical aspects of board governance as composition of the board, board structure, various committees, board powers, directors' responsibility statement, ceiling on number of directorships and committee memberships, and compensation of directors are covered by the relevant provisions of the Act. The Act has been amended 24 times since 1956 to reflect the ever-changing corporate landscape.

57.3 MINISTRY OF COMPANY AFFAIRS

The Ministry of Company Affairs also administers the Institute of Chartered Accountants of India (ICAI), set up under an act in 1950, and the Institute of Cost and Works Accountants (ICWAI) of 1950. The Company Law Board serves the functions of corporate courts in India. The Institute of Company Secretaries in India is the source of supply of qualified company secretaries in India.

57.4 SECURITIES AND CONTRACTS (REGULATION) ACT OF 1956

The Securities and Contracts (Regulation) Act of 1956 regulates the issue of various types of securities besides defining the parameters of conduct for the stock exchanges and their powers.

57.5 SECURITIES AND EXCHANGE BOARD OF INDIA (SEBI) ACT OF 1992

In 1992 the Securities and Exchange Board of India (SEBI) was created under an Act of the Parliament to provide a framework of corporate conduct. The government of India established the SEBI as an independent capital market regulator. One of the tasks before the SEBI is investor protection; other tasks are

promoting and regulating securities markets and also monitoring the conduct of market intermediaries. Due to corporate scandals in the closing decades of the twentieth century the SEBI and Ministry of Finance appointed a number of task forces to suggest ways and means of improving corporate governance; the first formal code was issued by the CII 1998, followed by the Birla Committee 2000, Narayan Murthy Committee 2003, Naresh Chandra Committee 2002, and J. J. Irani Committee 2005. The RBI had constituted in 2002 advisory groups as a part of the Standing Committee on International Financial Standards and Codes (Ganguli Committee). These committees have adopted codes of corporate governance evolved by (and since) the Cadbury Committee (UK 1992) and those of the others countries, more notably, the United States, Canada, Australia, and Europe, among others. Besides, multilateral institutions such as the World Bank, the Organization for Economic Cooperation and Development (OECD), the International Monetary Fund (IMF), the Asian Development Bank (ADB), and others have also formalized generic codes of corporate governance, which may be adopted with some modifications in countries the world over.

57.6 DEPOSITORIES ACT OF 1996

The Depositories Act of 1996 set up depositories and provided a framework for dematerialization of shares.

57.7 ACCOUNTING STANDARDS

The accounting standards required to be complied with for preparation of financial statements and for an overall counting policy framework of companies are the standards that are recommended by the Institute of Chartered Accountants of India and are prescribed by the central government in consultation with the National Advisory Committee on accounting standards constituted under Section 210 A(1). India's accounting standards are derived from the International Accounting Standards. The Indian firms that have raised funds from the U.S. markets are required by the Securities and Exchange Commission's regulations to translate their financial statements as per the U.S. Generally Accepted Accounting Principles (GAAP) or to prepare reconciliation statement reflecting the difference between Indian GAAP and the U.S. GAAP.

57.8 LISTING AGREEMENT OF THE SEBI 2000

Clause 49 of the Listing Agreement was incorporated in 2001 for the listed companies in the BSE and new companies with paid-up capital of 30 million rupees (US$660,000) or with a net worth of 250 million rupees (US$5.5 million) at any time in the past five years. Some revisions in Clause 49 were proposed in 2003 but were actually not introduced during the period. In the postliberalization period the focus was on market-oriented reforms and improving the competitiveness of the Indian industry. Since the recommendations of the SEBI committees

and other task forces in India, there has been some debate on the role of independent directors. Clause 49 of the Listing Agreement was revised in 2004 and subsequently in early 2006.

The companies listing their securities with the stock exchanges are required to comply with various clauses of the Listing Agreement in order to continue to be listed. Clause 49 provides a specific framework of rules for corporate conduct with a view to intiaite and sustains higher standards of corporate governance. In addition, companies in the sectors such as banking, insurance, and finance are subject to rules and regulations as contained in the specific legislations from time to time.

57.9 GENESIS OF CLAUSE 49

The SEBI in India has initiated several measures to strengthen the statutory framework for streamlining the functioning of the stock exchanges, issuers of securities, and issue intermediaries. Based on the recommendations of the Kumar Managalm Birla Committee of 1999, the SEBI introduced Clause 49 and the stock exchanges were required to incorporate Clause 49 relating to corporate governance in the Listing Agreement as of the financial year 2003. Subsequently on the basis of the recommendations of the Naresh Chandra Committee of 2002 and the Narayan Murthy Committee report, Clause 49 was revised in 2004 and December 2005.

The revised clause is applicable to all the companies listing their securities for the first time. The existing companies that were complying with the provisions of the earlier clause are bound by the revised code. Clause 49 consists of two provisions: mandatory and nonmandatory. The nonmandatory provisions are more a set of guidelines and are provided to initiate companies into self-regulatory behavior. Clause 49 deals with the specific aspects of corporate governance such as board composition, board structure, and disclosures, among others.

57.10 MANDATORY REQUIREMENTS

In what follows we provide an overview of the mandatory requirements together with specific implications for the companies.

(a) CLAUSE 49(I)(A): BOARD COMPOSITION. This provision deals with two very critical issues of corporate governance; the first is the CEO duality, a situation wherein the role and position of chairman and CEO are combined; the second deals with the issue of balancing board composition in terms of experience, expertise, and authority by way of inducting independent directors. According to the stipulation in case of CEO duality, the board shall consist of a minimum of 50 percent of independent directors, while in the case of nonduality the board shall have a minimum of one-third of independent directors. The definition of independent directors adopted for the purpose of board composition is the most generic

practice as already prevalent worldwide. The definition of independent directors includes the following prerequisites:

- Does not have any pecuniary relationship with the company or its directors, promoters, senior management, or its holding company, subsidiary companies, or associates
- Is not related to promoters or persons occupying management positions at the board level or one level below the board level
- Has not been an executive of the company during the previous three years
- Is/was not a partner or an executive during the previous three years of the statutory or internal audit firm associated with the company, and legal/consultancy firms that have material association with the company
- Is not a material supplier, service provide, customer, lessor, or lessee of the company that may affect independence
- Is not a substantial shareholder holding 2 percent or more of the stock of voting shares

The tenure of independent directors may not exceed a total of nine years (three terms).

(b) CLAUSE 49(I)(B): COMPENSATION OF NONEXECUTIVE DIRECTORS AND DISCLOSURES. The compensation of the nonexecutive directors shall be determined by the board of directors before its approval by the shareholders at the general meeting. The shareholders' resolution must specify the limit on the number of stock options that can be granted to the independent directors. As for the sitting fees, if the same are within the prescribed limits as laid down by the Companies Act of 1956, prior approval of the shareholders is required. The responsibility of administering employee stock options scheme and employee stock purchase scheme guidelines of 1995 must be entrusted to a compensation committee.

(c) CLAUSE 49(I)(C): BOARD COMMITTEES. Under section 291 of the Companies Act of 1956 the board may delegate some its powers to its own committees. Clause 49, however, forbids a director from being the chairman, and a member of more than five and ten board committees respectively of public companies listed or unlisted. For the purpose of these limits, only the audit committee and shareholder's grievance committees shall be taken in to account. Each director should submit annually information on such position and the change therein.

(d) BOARD MEETINGS. As per the Companies Act of 1956 and Clause 49 there is uniformity of provisions regarding the minimum number of board meetings, but in respect to the gap between any two meetings the provisions differ.

(e) CLAUSE 49(I)(D): CODE OF CONDUCT. On the pattern of Section 406 of the Sarbanes-Oxley Act of 2002, (U.S.), the boards in India are required to lay

down a code of conduct for board members, senior management, and those one level below the executive director and the functional heads.

The compliance to such a code must be confirmed by the CEO by way of declaration that is to be included in the annual report; and in case of noncompliance the report should contain the reasons thereof.

(f) CLAUSE 49(II): AUDIT COMMITTEE. The listed companies are required to set up an audit committee consisting of a minimum of three directors; at least two-thirds of its members must be independent directors. At least one of the members must have accounting related financial management expertise. Such an expertise may be in terms of experience in finance, or accounting, or a professional qualification; or by virtue of being or having been a CEO, CFO, or other senior officer with financial responsibility. The committee shall be headed by an independent director. The committee chairman should be present at the Annual General Meeting (AGM). The committee may invite senior executives in the meetings or may meet without them. Section 292(A) makes it compulsory for the finance director and head of internal audit to participate in the meetings but these officials do not have a right to vote. The committee should meet at least four times a year, and the time gap between two meetings shall not exceed four months. The powers of the audit committee under Section 292 A(7) of the Companies Act 1956 and Clause 49 are also similar. These powers extend to the investigating of any item or activity specified in the provision or falling within the terms of reference referred to it by the board. The committee shall full access to all records, seek information from any employee, and/or obtain outside legal, professional, or external advice. The audit committee's functions include: adequacy of internal audit function; a review of financial statements; changes in accounting policies or rules, compliances, disclosures, and qualifications in the draft audit reports; adequacy of internal control system; review of the whistle-blower mechanism, among others. The committee has the powers to appoint, replace, and remove statutory auditors and determine the audit fees.

(g) DISCLOSURES. Disclosures and transparency are the most crucial components of corporate governance. Some of the important considerations are: disclosures' costs should not be prohibitively high; they should not compromise the competitive position of the enterprise; and the disclosures should be made with reference to materiality. In particular, such disclosures as the related party transactions, accounting treatment, risk management, utilization of funds, remuneration, management discussion and analysis report, disclosures by senior management, and disclosures of particular directors, among others, are very important for an effective process of corporate governance.

(h) CLAUSE 49(V): CERTIFICATION BY CEO/CFO. The CEO and CFO must submit affirmations regarding a review of financial statements and cash flow statements.

(i) CLAUSE 49(VI)

(i) Report on Corporate Governance. The listed companies should include in the annual report a compliance report on corporate governance.

(ii) Evaluation. There are critical issues in initiating reforms on matters of corporate governance such as: multiplicity of regulators, inadequate deterrence, lack of harmonization of various enactments, a box-ticking mind-set of company management, and overreliance on independent directors for improving corporate governance process, among others.

One of the most critical issues is the recruitment and selection of independent directors; there is a supply constraint and also an absence of training infrastructure. The agency problems in the tripartite relations among the shareholders, board, and the top management are often compounded by the domineering attitudes of the promoters, especially in family-owned businesses. In the case of the listed Indian public enterprises, the recruiting agency has not taken enough steps to select an adequate number of independent directors and in many instances the nonexecutive directors who are nominees of the controlling ministries are made members of the audit and other board committees, which is contrary to the SEBI guidelines. Also, the moot point in the emerging corporate landscape in India is whether excessive legislation and regulation are making the companies more compliance reoriented as against governance oriented.

The supply constraint affects adversely the composition and the functioning of the board committees. A compensation committee is not mandatory, but as per Schedule XVIII of the Companies Act of 1956, the formation of such a committee in loss-making companies is mandatory. In view of the large number of companies in India, it is not possible for any single agency to sustain an enforcement framework; but certainly better harmonization of rules and purposeful enforcement would go a long way in improving investor confidence in the process and content of corporate governance.

It is also not ascertainable if a significant number of companies have evolved or adopted an audit committee charter. It is the responsibility of the audit committee as also the full board to ensure that there is a charter and it is adhered to. In a number of cases also there are issues of relations between the auditing firms and the companies that need to be sorted out by the board.

Despite various amendments in the Companies Act in 2003 and the revision in Clause 49 there is a need to review some of the nonmandatory clauses such as: separation of the roles of CEO and chairman, compensation committee, shareholder grievance committee, ethics committee, and the nomination committee. A significant number of companies continue to be without such committees, and in such a context the current limitations of corporate governance practices in India do not adequately create, let alone sustain, shareholder value.

The amendment in the legal and regulatory framework alone cannot create a mind-set that is value creating. Of course, it is necessary that the companies

comply with the legal and regulatory provisions, but the more crucial step is once they comply in what specific manner they may be encouraged and motivated to move beyond a compliance orientation. It is a larger perspective of the evolving financial markets and business systems that will contribute toward fine-tuning the corporate governance process and content in the long run. One of the challenges is to create an investment climate in which there is no fear of the enforcer but a certain degree of respect and regard; and this can be done only by evolving an appropriate public policy for corporate governance.

References

Desirable corporate governance: A code of confederation of Indian industry. April 1998.

Report of SEBI (Securities and Exchange Board of India) committee on corporate governance. February 8, 2003.

Report of the advisory group on corporate governance, standing committee on international financial standards and codes (RBI) March 2001.

Report of the committee (Kumar Mangalam Birla) on corporate governance. May 7, 1999.

Report of the committee on regulation of private companies and partnership, Naresh Chandra Committee-II (Ministry of Finance and Company Affairs). July 2003.

Report of the joint committee on stock market scams and matters relating thereto. Vol. 1. December 2002.

Report of the Naresh Chandra (Ministry of Finance and Company Affairs) on corporate audit and governance. December 23, 2002.

Report of the RBI advisory group on securities market regulation. 2000.

Report of the task force on corporate excellence through governance (Department of Company Affairs). November 20, 2000.

Sarbanes-Oxley Act of 2002. January 2002.

Sithapathy, V., and Ramadevi R. Iyer. 2006. *Corporate governance: Practice and procedures*. n.p.:Taxman and Allied Services Pvt. Ltd.

World Bank. 2004. Report on the observance of standards and codes (ROSC): Corporate governance country assessment—India. April 2004.

CHAPTER 58

CORPORATE GOVERNANCE: AN OVERVIEW ON THE ITALIAN CASE

Marco Venturini
Francesca Bevilacqua

58.1 INTRODUCTION

The recent financial scandals in Italy, such as Parmalat, Cirio, and Telecom have led to an increasing attention on corporate governance, the system of rules and practices aimed at ensuring the efficient, effective, and ethical corporate activities.

As a consequence, the interest generated by the area of corporate governance has led to the need for a more appropriate and exhaustive system of laws and controls.

In this chapter we try to analyze the Italian capitalistic model, the evolution of the corporate governance within this scenario, and the current legislation in Italy.

(a) THE ITALIAN CAPITALISTIC MODEL. A survey carried out by Banca d'Italia in 2001 shows that the most representative enterprises in the Italian capitalistic model are small and medium companies, in which the owner, the shareholder, and the manager are often the same person. Even if this kind of company, with its simplified legal structure, is the most common and characteristic in

the Italian capitalistic model, there is a wide variety of other enterprise structures that exist:

- Small and medium family enterprises
- Small-medium enterprises organized in clusters and localized in particular areas
- Big groups controlled by a family or by shareholders' coalitions
- Big companies or groups controlled by the government and local authorities
- Cooperatives and pools of companies
- Branches of multinational corporations

In this context we observe a lack of public companies (typical in Anglo-Saxon capitalism), and mixed financial and industrial groups (typical in German and Japanese models), which characterize the great part of other industrialized countries.

Research by Assolombarda and Bocconi University (2000) also confirms that most Italian companies have legal structures composed of a few shareholders (families, multinational groups, government, or local authorities), which are able to influence the board of directors. The research also finds that companies controlled by financial or insurance institutions are less common.

Since the second half of the 1990s, the divestments in particular businesses by big families and the process of privatization promoted by the government have been paving the way for an increasing presence of public companies. As a consequence of this trend and of the recent financial scandals, more attention has been paid to corporate governance issues by politicians as well as managers and institutional investors.

(b) THE EVOLUTION OF CORPORATE GOVERNANCE IN ITALY. In the recent past, the prevalent theory on corporate governance concerned shareholder value (maximization of the value per share in the short term), while most recent studies show that more attention is paid to the long-term value for all the stakeholders. In the past, corporate governance was intended as the system of rules to regulate principal-agent[1] conflicts, while today it is largely accepted that its main task is to protect all the stakeholders from management's opportunistic behaviors, supporting the creation of value in the long term.

Corporate governance is a widely discussed, complex, and difficult concept which is very important, but not easy to define. We can try to arrange a framework, considering the corporate governance role from two points of view: an institutional one (which concerns all factors external to the company) and a managerial one (which concerns the internal operations).

From an institutional point of view, corporate governance is intended as a set of rules, institutions, and procedures external to the company aimed to protect investors from opportunistic behaviors by owners and managers and to ensure an

adequate return on their investments. From a managerial point of view, corporate governance is focused on the procedures through which management organizes and manages the company resources, influencing the value creation process.

58.2 THE INSTITUTIONAL POINT OF VIEW

Under Italian law two main types of company may be incorporated: S.p.A. (Società per Azioni) and S.r.l. (Società a responsabilità limitata).

S.p.A (Civil Code, Section 2325 ff.) is the normal form for larger companies (joint stock companies). An S.p.A. may be listed on the Italian stock exchange, although the absolute majority are not. It is, however, necessary for a company to be an S.p.A. in order to be listed thereon.

S.r.l (Civil Code, Section 2472 ff.) in practice corresponds to a closely held limited company. It is the kind of structure that is more suited to small to medium-sized enterprises where limited liability is required. This is by far the most common type of company used by Italian entrepreneurs and that most frequently chosen by foreign parent companies when setting up their subsidiaries in Italy.

(a) CORPORATE GOVERNANCE IN S.p.As. The traditional structure of Italian companies is based on a clear-cut distinction between different functions assigned to three separate bodies:

1. *General meeting of shareholders*, which is responsible for approval of the balance sheet, the appointment of directors, and the determination of remuneration for directors and statutory auditors.
2. *Directors*, an organ that may be represented by a sole director or by a board of directors and is in charge of management.
3. *Board of statutory auditors*, which invigilates on compliance by the company management with the law and the articles of association, on respect by the management of rules of correct business administration, as well as on the adequacy of the company's organization and accounting and on its actual operation. According to the reform, statutory auditors will no longer control the company accounts, a function that is now exclusively entrusted to external auditors.

The reform has introduced two alternative management and control systems, recommended by the EU Council Regulations on the European Company By-Laws dated October 8, 2001:

The *dualistic system* (s. 2409 ff., Civil Code), deriving from the German/French experience, provides for:

- A management board, which has the same kind of responsibilities as those attributed to the board of directors

- A supervisory board with wider tasks than those of statutory auditors, including appointment and revocation of management board members and approval of the company's accounts

The supervisory board is also exclusively enabled to promote actions in liability against members of the management board and to waive such actions by way of settlement out of court. Consequently, in a company managed in accordance with this two-tier system, the functions of the shareholders' meeting are confined to appointing and revoking members of the supervisory board.

According to the *monistic system* (s. 2409 sexiesdecies ff. Civil Code), deriving from English experience, management is entrusted to a regular board of directors (at least one-third of these directors must be independent[2] members), while supervision is attributed by the board to a management control committee (its members are chosen among independent directors).

The number of members of such committee is determined by the board. In companies that make recourse to the capital market, the committee must be constituted by no less than three members.

(b) CORPORATE GOVERNANCE IN S.r.ls. In the view of the legislature, an S.r.l. should be the most flexible tool in the hands of shareholders.

In line with this very flexible structure, the managing body of an S.r.l. may be freely shaped by shareholders by way of recourse to some alternative solutions:

- A sole director
- A traditional board of directors collectively acting as a committee, presided over by a chairman and by a managing director
- A board of directors not acting as a committee, formed by a plurality of members having the same powers

Supervision of accounts will be entrusted to a board of statutory auditors or to a sole auditor only where the company share capital is in excess of €120,000 or when the turnover or the size of an S.r.l. is beyond a certain threshold determined by law.

An important contribution to identifying the fundamental elements to establish effective corporate governance was the 1996 "Corporate Governance Project for Italy."

Its scope was to adapt the U.S.-based COSO Report (Committee of Sponsoring Organizations, 1992) on internal control and to further examine the roles, responsibilities, and processes of various players (shareholders, directors, supervisor bodies, external audit companies, and other stakeholders).

Many of the issues arising from the Project were then resolved via the reform introduced by the Draghi law on corporate governance, which came into force in 1998, while certain corporate governance principles have been stated in

subordinate legislation, particularly by the implementing regulations issued by Consob (Commissione Nazionale per le Società e la Borsa: Supervision Committee for listed companies).

A further and fundamental contribution in the Italian context was the Code of Conduct for listed companies, issued in October 1999 by Borsa Italiana S.p.A. and also known as the Preda Code.

58.3 THE MANAGERIAL POINT OF VIEW

The new Italian legislation gives considerable importance to internal controls, a focal point of Code of Conduct, which states that "the internal control system is charged with the task of checking effective compliance with the operational and administrative internal procedures adopted to guarantee an efficient management and to identify, forestall and limit, as far as possible, financial and operational risks and fraud at the company's expense."

In this way, the Code of Conduct underlines that internal control procedures represent an integral part of corporate procedures and as such form part of the organizational structure. (See Exhibit 58.1.)

In order to better understand the evolution of internal control procedures it is helpful to examine the main differences between the traditional and the modern approach to internal control:

- *Policy and communication of objectives*. From a traditional point of view, the main objective is to demonstrate compliance at minimum cost within a context characterized by a lack of control culture at all levels.

  In contrast, the modern approach is based on risk identification and on controls that are fundamental to business management. In this context, the control culture expresses the company's style and internal philosophy and has the main scope of being made known at all levels of the organization.

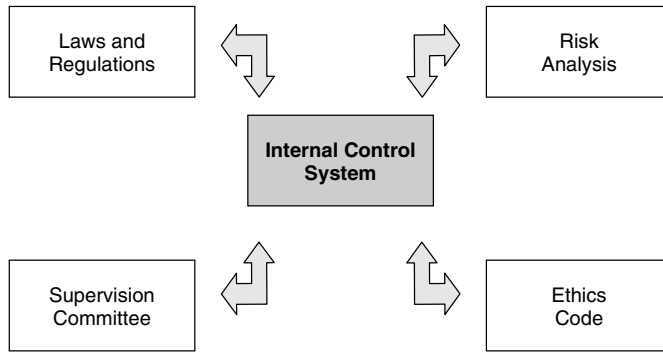


EXHIBIT 58.1 THE INTERNAL CONTROL SYSTEM MODEL

- *Accountability*. In the traditional approach accountabilities are assigned on the basis of rigid systems, which are often not changed over time and there is no knowledge of the accountabilities assigned to the other business areas.

  In the modern approach, roles and accountabilities are assigned on the basis of the definition of objectives. Each individual must be clear as to his accountability and his involvement in achieving business objectives. Basic to the modern approach is clarity in defining and communicating roles at all levels.
- *Risk assessment and planning*. The traditional approach is characterized by risk identification only in sensitive situations and the planning and risk assessment process is limited to top management.

  The modern approach is characterized by a process for the identification and assessment of risks that significantly threaten the business objective and the board of directors defines the philosophy, but the process is propagated through the organization. The identification of business objectives leads to the assessment of all possible related risks.
- *Capability*. The traditional approach is based on inflexible career paths and limited monitoring to identify resources within the organization; knowledge and learning about risk management and control issues are limited to few people.

  The modern approach stresses career planning processes responding to the company's specific internal needs, the optimization of resources management throughout the organization, and the creation of a supportive environment for training and learning about risks and control issues.
- *Overall process review*. In the traditional approach, the board of directors views internal control passively and ensures that the system is in line with the requirements of relevant legislation, the internal audit reports are prepared for extraordinary events, and the finance/administration function is in charge of the internal control system.

  In the modern approach the board of directors/audit committee views internal control actively. The development of the continuous monitoring process, which is inherent to business operations, provides management with regular reports on the status of internal control system. The top management actively supports the control activities.

These comparisons show the evolution of the control concept in corporate governance and demonstrates how important it is in a context of continuous change in organization and business conditions: in Italy, 231/01 Law has represented a fundamental step because it compels the company to adopt an internal control system (*modello di organizzazione*, *gestione e controllo*) and to introduce a supervision committee (*organismo di vigilanza*).

When the Law was introduced in 2001, it was only concerned with offenses against the public sector, while at present it concerns all the kinds of corporate offenses (market abuse, individual violations, etc.).

The main sanctions provided by the Law can be classified in two main types: cash and disqualification penalties. These penalties occur only if the company can not demonstrate that an internal control system has been implemented and that a supervision committee has been adopted.

58.4 CONCLUSION

Corporate governance has generated intense interest in the past few years, with particular attention to the area of protecting socially relevant interest, as it has among large Italian groups, which capitalize on the opportunity to protect stakeholders and to create added value for them through good corporate governance.

Many efforts have been made by the Italian government and market authorities in order to promote and implement laws and best practices. These efforts have certainly represented a significant step to make the Italian situation increasingly comparable to and competitive in the international context.

This is only the first step of a process that still has to demonstrate its effectiveness. Therefore only a few companies have adopted modern internal control systems. Few have developed a transparency and compliance culture, and recent financial scandals, such as Telecom, have shown that a lot still remains to be done.

Notes

1. The "agency theory" is aimed at optimizing the relationship between two subjects (principal and agent): the manager (agent) who accepts to operate on behalf and in the interest of another subject, and the owner (principal) who delegates to the manager (agent) the decisional authority on specific duties and activities. The agency theory tries to identify the controls, incentives, and risk-sharing systems able to maximize the economic relationships efficiently.
2. The concept of independent members, according to the Code of Conduct issued by the Committee for Corporate Governance of Listed Companies, Italian Stock Exchange (Borsa Italiana): Members are considered independent when they do not entertain business relationships with the company, its subsidiaries, the executive directors, or the shareholders who control the company of a significance as to influence their autonomous judgment; they do not own directly or indirectly a quantity of shares enabling them to control the company or participate in shareholders' agreements to control the company.

References

Albet, Josep., "Guida pratica alla corporate governance. Egea.," Aegean Press, 2006.

Atti del convegno. Donne e governance. Governance Consultino, Milano, October 2006.

Banca d'Italia. 2001, http://www.bancaditalia.it/.

Il Sole 24 Ore, Università Bocconi. 2006. Corporate governance, management.

KPMG Audit. 2001. Corporate governance in Italy: A practical guidance to internal control.

La Rocca, Maurizio. 2005. Manager e Azionisti: Evidenze empiriche e problemi aperti nella prospettiva della corporate governance. SDA Bocconi, Economia e Management.

Zattoni, A., and D. Ravasi. 1998. Assetto proprietario, sistemi di governo e processi di decisione strategica nelle imprese con controllo di coalizione. In G. Airoldi and G. Forestieri (a cura di), *Corporate governance: Analisi e prospettive del caso italiano*. Milano: Etas Libri.

CHAPTER 59

THE GUIDE TO GLOBAL COMPLIANCE: THE NATIONAL CHAPTER—JAPAN

Kouji Yamamoto

59.1 INTRODUCTION

After the meltdown of the so-called bubble economy in 1992, the Japanese government boosted the Japanese economy by easing regulations and reforming the tax system. These changes led companies to change their business styles and try to expand their markets, which resulted in intense competition. Companies were, and still are, forced to compete for their very survival. Because of this stressful business environment, management may naturally tend to view

compliance as just another problem. However, even though there are many difficulties associated with it, compliance is critically important to the future stability of companies worldwide.

Compliance does not just mean obeying laws or following the regulations of a company. It also means following the ethical code that each company sets for itself. Despite showing interest in compliance year after year, most boards of directors and corporate officers have not yet taken concrete and effective measures to realize compliance.

However, recent changes in Japanese corporate law have clearly outlined the legal responsibilities of boards of directors and corporate officers in the area of compliance. These recent changes also specify that the legally required method of achieving compliance is internal control. Internal control is defined as a process, managed by an organization's board of directors, management, and other personnel, which is designed to provide reasonable assurance of an organization's ability to achieve four objectives:

1. Effective and efficient operations
2. Reliable financial reporting
3. Compliance with applicable laws and regulations
4. Safeguards

There are six components of internal control that work together to enable a company to achieve compliance. These six components are: control environment, risk assessment, control activities, information and communication, monitoring, and utilization of IT (information technology).[1]

Management must first determine the desired level of internal control based on the amount of risk they are willing to accept. Then they must assess the current status of the six internal control components within their company. Finally, if any of these components are insufficient or lacking, management must make the necessary changes to ensure that all six components are in place and functioning properly, as dictated by the desired level of internal control.

59.2 CURRENT STATE REGULATORY COMPLIANCE OVERVIEW

(a) POLITICAL AND CULTURAL ENVIRONMENT. The Japanese government has started to deal with many cases of financial fraud (which will be discussed later) and has introduced some laws concerning compliance. These changes were necessary to raise the compliance level of Japanese companies and received a great deal of political support.

Japanese people are very hardworking and Japanese culture is top-down. Once a rule is implemented, it will be followed. However, most of the laws only set down basic ideas, without any concrete guidance as to how to apply them in the real world. Therefore, most Japanese companies are waiting to see what will happen next.

(b) LEGAL ENVIRONMENT. In Japan, two major new laws went into effect in 2006. One is the new Corporate Law, and the other is the Financial Instruments and Exchange Law. The new Corporate Law was reorganized from the former Commercial Law that was established in 1899 and was based on German Commercial Law. The new Corporate Law's objective is to regulate commercial transactions and balance the conflicting interests of creditors and stockholders.

The Financial Instruments and Exchange Law was established by reorganizing the Securities Exchange Law, based on the Securities Exchange Act (1933, 1934) in the United States. The Financial Instruments and Exchange Law's objective is to control the issuing and trading of financial instruments and to protect investors. Because of this extensive reorganization, Japanese corporate accounting is a hybrid of German and American accounting theories.

(i) New Corporate Law. The new Corporate Law, which took effect on May 1, 2006, requires that a company's board of directors take responsibility for the primary development and implementation of internal control. Management is required to introduce and utilize internal control to achieve compliance. This internal control covers the four objectives discussed on the previous page, and is broader than the idea of internal control covered under the Financial Instruments and Exchange Law, which is concerned only with reliable financial reporting. Management must proceed with care because the new Corporate Law does not specifically outline the necessary level of internal control for a company. Because all companies are different, the level of internal control will, of course, differ from company to company. Management must ensure that the company has adequate internal control in place, because if any problems occur due to inadequate internal control, the board of directors could be vulnerable to legal action.

(ii) Fraudulent Financial Reporting. As stated previously, after the meltdown of the bubble economy, companies were forced to compete for their very survival. Mutual shareholding[2] was discouraged and corporate realignment was promoted. As a consequence, many cases of financial fraud occurred. In one case, Seibu Railway Co., Ltd.[3] intentionally misstated the percentage of its stock held by Kokudo Planning Co., Ltd, its parent company. Had Seibu Railway reported the correct percentage, it would have been delisted from the Tokyo Stock Exchange.

In another case, Kanebo, Ltd.[4] took advantage of vague consolidation criteria as well as business combination rules that were not well developed. Kanebo intentionally did not consolidate 15 deficit-ridden companies, and merged three companies that held depreciated property to offset profits of another merged company. Kanebo also sold dead inventory to distribution outlets by push operation at the end of the fiscal year. In addition, Kanebo carried over advertising costs and sales promotion costs into the next year in order to overstate profits and sales by 200 billion yen from 1999 to 2003.

In the most recent case, Livedoor Co., Ltd.[5] manipulated its stock price through fraudulent transactions and misinformation. Livedoor sold its own shares

at a high price by using business investment associations and recognized this as profit rather than as a capital transaction.

As these examples demonstrate, because of collusion or improper override of internal controls by management, material misstatements due to error or fraud may not be prevented or detected in a timely manner. To prevent fraudulent acts, it was necessary for the Japanese government to take into consideration more effective measures, such as the introduction of severe criminal penalties or the adoption of a strict auditing approach in order to uncover cases of fraud. In Japan, many boards of directors and corporate officers still have only a superficial understanding of the importance of internal control and compliance, mainly due to the absence of severe criminal penalties.

(iii) Financial Instruments and Exchange Law. The Financial Instruments and Exchange Law consists of three stages, with the first two being of notable significance. The first stage, covering changes in the severity of criminal penalties, took effect as of July 4, 2006, tightening regulations on fraudulent financial reports, misinformation, and manipulation of stock price. It provides for a maximum of 10 years' imprisonment or a fine of up to 10 million yen or both for management, but these penalties are still not as severe as penalties in the United States.

The second stage, which will come into effect on April 1, 2008, will require a company's management, including the chief executive officer (CEO), chief operating officer (COO), and chief financial officer (CFO) to assess the company's internal control over financial reporting. It also requires the company's CEO to prepare the Management's Report on Internal Control over Financial Reporting based on the results of this assessment. In addition, certified public accountants (CPAs) are required to audit the Management's Report on Internal Control over Financial Reporting prepared by the CEO.

(c) ACCOUNTING/FINANCE ENVIRONMENT

(i) Background. In the 1990s, Japan GAAP (generally accepted accounting practices) was about 30 years behind accounting principles generally accepted in the United States (U.S. GAAP). In order to realize a free, fair, and open financial market, the Japanese government decided to raise the standards of Japan GAAP with the introduction of major new accounting rules. Some of these dealt with tax allocation, statement of cash flow, financial instruments, pensions, impairment accounting, and business combination. In Japan, this was referred to as the "Big Bang" of accounting.

(ii) Japan GAAP. Currently in Japan, in addition to Japan GAAP, three major laws have an effect on Japanese accounting practices. These are the new Corporate Law (formerly the Commercial Law), the Financial Instruments and Exchange Law (formerly the Security and Exchange Law), and the Corporate Tax Law.

Article 193 of the Financial Instruments and Exchange Law requires a listed company to file financial reports with the Financial Services Agency as outlined

in Japan GAAP. Article 432 of the new Corporate Law requires a company to prepare financial reports, again as outlined in Japan GAAP, for the approval of stockholders. However, because of the global nature of business today, a company must recognize other international standards of accounting, which brings about the problem of convergence.

(iii) Convergence. Japan faces the problem of convergence between Japan GAAP, International Financial Reporting Standards (IFRS), and U.S. GAAP. To develop and revise accounting rules more quickly and effectively, authority over accounting standards was transferred to the Accounting Standards Board of Japan (ASBJ) from the Business Accounting Council and the Japanese Institute of Certified Public Accountants (JICPA). The ASBJ has held over 100 sessions dealing with new accounting standards and has issued more than 30 new accounting standards dealing with the problems of convergence as well as adjustments under the new Corporate Law. Some of these new standards are Related Party Disclosures, Inventories, and Revenue for IT.

(iv) Effect of Corporate Tax Law. The Corporate Tax Law requires a company to calculate its taxable income based on its final profit with the stockholders' approval. As a result, this and other rules that the Corporate Tax Law outlines have an effect on the accounting policies that companies adopt, such as the depreciation method, useful life, and residual value, when they prepare financial reports required by the new Corporate Law and the Financial Instruments and Exchange Law.

(d) AUDITING ENVIRONMENT. In Japan, the former Commercial Law outlined an Auditors System (similar to the German governance system) in which CEO-appointed auditors, under the authority of the board of directors, audited the actions of directors and officers. However, in the case of a large company,[6] CPAs were required to audit the accounting functions of the company. The CEO-appointed auditors were then required to evaluate the validity of the CPAs' audit, in addition to auditing the management and operation functions of the company. The new Corporate Law that succeeded the former Commercial Law contains the same system. In addition, in the case of a listed company, the Financial Instruments and Exchange Law also requires CPAs to audit the financial reporting of the company.

(i) Problems with the CEO-Appointed Auditors System. Under the CEO-Appointed Auditors System, there is a conflict of interest for most of the auditors involved because it is difficult for them to impartially audit the CEO and board of directors. They are not independent. Auditors had been empowered by changes in the former Commercial Law, but it was still difficult to say that the Auditors System functioned well. So, in 2002, the former Commercial Law was changed to introduce the Audit Committee System (American-type governance

system), which allows a large company to choose between the Auditors System and the Audit Committee System. When choosing, management should determine which system would best serve their company, taking into consideration their own unique corporate environment.

(ii) Problems with the CPA Auditing System. Now more than ever, the CPA Auditing System is in question. In the Kanebo case, CPAs from one of the major auditing firms in Japan advised Kanebo how to dress up its financial reporting. In the Livedoor and Seibu Railway cases, CPAs from medium-sized and small auditing firms could not detect or prevent misstatements.

These examples and others demonstrated that the problem was with the CPA Auditing System itself, rather than just with individual auditing firms. As a result, the Financial Instruments and Exchange Law and the Certified Public Accountant Law introduced new penalties for CPAs and strengthened existing ones. The Financial Services Agency also adopted penalties for CPAs. Subsequently, one major auditing firm was suspended for two months and a medium-sized auditing firm was disbanded.

(iii) Direction of Reform. The diversification, complexity, and globalization of the Japanese economy pose auditing risks due to the numerous types of fraud or other misstatements possible in financial reporting. Despite this, audit working time in Japan is currently about one-third to one-half of the audit working time in the United States, England, and Germany. This situation will have to change if Japanese CPAs wish to maintain a high level of professional quality and competently deal with the complexity of the new economy.

CPAs have the responsibility to maintain auditing quality by obtaining comprehensive and sufficient auditing evidence, carefully documenting the auditing process and results, reinforcing quality control, and conducting sufficient personnel training within auditing firms. As of April 1, 2008, CPAs will have the additional responsibility to audit a company's Management Report on Internal Control over Financial Reporting. Auditing time will naturally have to increase in order to maintain a proper level of quality and to handle the additional auditing responsibilities.

In order to promote and monitor auditing quality, the JICPA has introduced two measures. One of these, the Board of CPAs Review, was introduced as a quality control system to monitor the quality of audits carried out by Japanese CPAs. The JICPA has also decided to introduce the rotation system, so that CPAs now are not allowed to take charge of the same client for more than five consecutive fiscal years. However, as the number of lawsuits against CPAs is expected to increase, the new Corporate Law allows CPAs to sign a limitation of liability contract with a company as long as the company changes its bylaws to allow this.

(iv) Convergence of Auditing Standards. Recent Japanese auditing standards for financial reporting are directly copied from the International Standards on

Auditing (ISA). So, the convergence of those auditing standards has been effectively accomplished. However, the auditing standards for internal control, scheduled to take effect from 2008, still use terminology inconsistent with the auditing standards for financial reporting. In the near future, these differences will have to be resolved because international auditing standards for internal control will also be developed and converged with Japanese standards. In order to realize global compliance, accounting standards, auditing standards for financial reporting, and auditing standards for internal control must be internationally coordinated and universally adopted.

59.3 COMPLIANCE TRENDS: CHALLENGES AND OPPORTUNITIES

(a) CULTURAL AND POLITICAL. Japanese people have the belief that human beings are inherently good. Following this idea, management trusts in the loyalty of its employees and sees it as a negative thing to effectively spy on them by implementing internal control. Also even if management introduces internal control, they believe that it is simply one of the tools at their disposal used to manage the company. They find it strange that members of management themselves are assessed as part of internal control. Some of them are concerned that they might be assessed based on the quality of their business judgment. These misunderstandings impede the realization of compliance.

However, the section of the Financial Instruments and Exchange Law requiring management's assessment of internal control over financial reporting will take effect on April 1, 2008. The experience of carrying out this assessment will, it is hoped, help management to understand the importance of internal control. Japanese companies have the habit of following the crowd and are loath to behave differently or stand out. Therefore, if some companies change their thinking on internal control, it is hoped this will be the trigger for the majority of companies to change.

(b) LEGAL. The new Corporate Law, which came into effect on May 1, 2006, brings with it many changes in corporate governance in Japan. Two important changes that management must consider deal with the balance between stockholder and management interests and the newly clearly defined legal responsibilities of CPAs. In 1993, a change in the former Commercial Law made it easier for stockholders to take legal action against boards of directors by lowering the costs associated with stockholder litigation. However, some problems resulted from this due to the abuse of stockholder litigation. To counter this, the new Corporate Law changes the concept of board-of-director liability from one of absolute liability to one of negligent liability, which takes into consideration whether the board of directors follows the basic principles of responsible management. This new Corporate Law will be continuously updated by the Japanese government in order to maintain a balance between the protection of stockholder interests and management's freedom to use their best judgment without fear of unfair legal action.

Another important difference in the new Corporate Law clearly defines the legal responsibilities that CPAs bear when auditing companies. Highly detailed auditing standards limit a CPA's ability to exercise personal judgment, and as a result he or she might conduct an overly conservative audit to conform to these standards, without considering any accounting practices that are not explicitly contained in these standards. This overly conservative auditing can result in a considerable amount of money and time wasted. To deal with these problems of stockholder litigation and overly conservative auditing as well as to keep the company up-to-date with the many changes in the new Corporate Law, management should make sure that the people in their legal and accounting departments have solid experience and training.

(c) TECHNOLOGY. As stated previously, internal control covers a broad range of business activities, and the Japanese version of the Committee of Sponsoring Organizations (COSO) framework also stresses the utilization of information technology (IT). Therefore, a number of IT products related to internal control are currently available, which can be divided into two types. One type is related to documents,[7] such as documentation software (which helps in the preparation of documents) or documentation management software (which organizes documents and makes them easy to access). The other type is related to improving internal control.

One example of software that helps to improve internal control is a whistle-blowing system. This kind of software system provides an e-mail function that all employees may use to contact internal auditors. All e-mails are anonymous, and the system also keeps a history of any actions internal auditors take in response to these e-mails. Another example of improving internal control is an auditing system. This kind of system allows authorized personnel (CEO-appointed auditors, internal auditors, tax inspectors, CPAs, etc.) to obtain information they need, such as audit trails, changes of log slips, data flows, data downloads, online screen information, and so on. This ability to obtain information quickly and easily helps in the preparation of timely and accurate audits. However, there are some IT products on the market that are not really useful for internal control but are just labeled "For internal control purposes," taking advantage of the current popularity of internal control. Management has the responsibility to first assess their current IT assets and to ensure that they are being utilized in the best possible manner for internal control. Second, if purchasing a new internal-control software system is necessary, management must be careful to choose the most effective, comprehensive, and cost-efficient one available, based on the company's needs.

(d) PROCESS. As of April 1, 2008, when the Financial Instruments and Exchange Law takes effect, management will be required to assess their company's internal control over financial reporting.

However, management at most listed companies in Japan have only recently started to prepare for these assessments. In the process, they have uncovered

many problems related to the business processes of internal control (for example procedures, controls, supervision, etc.) and have undertaken measures to correct these problems. All of these problems must be dealt with before management can evaluate, test, and report on the internal control over financial reporting at their company. Therefore there should be sufficient time to allow management to determine if the corrective measures they have implemented have been successful.

In order to efficiently develop and change business processes, management should take into consideration the seven Business Process Reengineering (BPR) principles:

1. Elimination of unnecessary processes
2. Simplification of complicated processes
3. Enforcement of company regulations
4. Efficient allocation of employees
5. Equalization of workload between busy periods and slow periods
6. Standardization of work
7. Utilization of automated systems

These principles provide management with a clear list of possible solutions they should consider, in order, when choosing effective measures to deal with problems related to internal control. Given the deadline of April 1, 2008, members of management have a limited amount of time to deal with the problems they have already encountered or will encounter in the future. Following the list of BPR principles in order from 1 to 7 will help them to overcome these problems more quickly and efficiently.

(e) PEOPLE. Up to now in Japan, employees have not had a clear understanding of the concept of internal control. Even if they were aware of fraud or other serious problems in their company, there was no system in place that would allow them to report this information without fear of reprisal. Currently, whistle-blowing systems in Japan are evolving and it is hoped that this situation is changing.

Whistle-blowing is important because it can provide the company with early detection of internal control violations, help reduce losses resulting from such violations, and also help reduce stockholder litigation. However, there are two major problems management must consider when establishing a whistle-blowing system. One problem is fraud committed by management itself, and the other is unfair treatment of employees who come forward as whistle-blowers.

The recent case of Livedoor is a good example of management fraud. In November 2005, a former officer of a Livedoor subsidiary blew the whistle on Livedoor's selling of its own shares on the stock exchange and subsequent improper recording of this transaction as profit. This triggered a criminal investigation. In the case of management fraud, since we of course cannot expect management to deal with the situation properly, whistle-blowers must report the situation to a proper outside authority.

Another problem with whistle-blowing is reprisal against those employees who are brave enough to come forward. In recent years, some indicators of fraud, such as some automakers' failure to properly report recalls to the government, or some food companies' deceptive labeling of food origins, were revealed by whistle-blowers. As a result, some of these whistle-blowers were fired or otherwise unfairly treated. As a consequence, from April 2006, a new law took effect for those who disclose information in the public interest. This law has the purpose of protecting whistle-blowers in cases related to the public interest, such as danger to human life, environmental protection, or fair competition. Overall, this new law protects whistle-blowers who report violations relating to 417 different laws and regulations.

To ensure effective internal control in the future, management must protect the interests of employees who come forward as whistle-blowers. The safer employees feel, and the more they are made to understand the importance of compliance, the more they will be willing to report violations of or deficiencies in internal control.

59.4 THE MARKET AND HUMAN BENEFITS OF GETTING THERE SOONER RATHER THAN LATER

The establishment of internal control provides many benefits to the market and to individuals as well, such as employees, stakeholders, and customers. However, it is difficult to measure these benefits until a problem arises, and a monetary loss is incurred, as the following two examples illustrate.

(a) THE MARKET BENEFITS. In December 2005, at Mizuho Securities Co., Ltd., a trader mistakenly entered a sales transaction for 610,000 shares at 1 yen per share, when it should have been a transaction for 1 share at 610,000 yen per share. The trader immediately tried to cancel this transaction, but he was unable to do so because of system problems at the Tokyo Stock Exchange. As a result, Mizuho Securities incurred a loss of 40.7 billion yen. Mizuho Securities maintains that this loss occurred because of the gross negligence of the Tokyo Stock Exchange.

Shortly after this incident, an additional system problem occurred at the Tokyo Stock Exchange due to increases in the volume of security transactions. This situation caused the shortening of trading hours for several months and affected the stability of the securities market. As a result, the Tokyo Stock Exchange is in the process of improving its system to prevent these kinds of problems from reoccurring, which will result in a smoother-functioning and more stable securities market.

(b) THE HUMAN BENEFITS. In June 2006, Tachibana Securities Co., Ltd.[8] also suffered a loss of over 1 billion yen because of an incorrect transaction. Despite what had happened at Mizuho Securities, management had not taken any effective preventive measures to decrease traders' mistakes. Traders are human beings, and human beings inevitably make mistakes. These mistakes often result in negative

consequences for the employees, such as official reprimands, loss of salary, loss of promotion opportunities, demotion, or even termination. Furthermore, if the company suffers serious damage or losses, this can result in job losses and damage to the local economy, especially if the company is forced into bankruptcy. Particularly after the Mizuho incident, Tachibana's management should have established adequate internal control to prevent such errors. The implementation of internal control as a preventive measure protects employees by reducing the risk of violations of compliance and helping to prevent the negative consequences of these violations.

59.5 CASE STUDIES

(a) LESSONS LEARNED. The case of Tachibana Securities, as well as many other past cases of violation of compliance, demonstrates that most problems that occur in a company are caused by a lack of adequate internal control. Even if a company has all the necessary elements of internal control in place, if the people involved do not fulfill their responsibilities, internal control cannot function properly. Seibu Railway, Kanebo, and Livedoor all had boards of directors and auditors, but still failed to protect themselves from serious violations of compliance.

Among the components of internal control, the control environment is especially important. The control environment sets the tone of the organization and promotes the awareness of the importance of internal control among employees. When management implements internal control, they should pay particular attention to control environment factors, such as positive corporate culture, participation of the board of directors, independence of auditors and CPAs, integrity and ethical values, and assignment of authority and responsibility.

(b) BEST PRACTICES. In February 2006, Taiyo Yuden Co., Ltd., a manufacturer of ceramic capacitors, dismissed its CEO, who had misused company funds to pay for excessive entertainment at Japanese inns and hot springs. Based on information provided by a whistle-blower, auditors had investigated the situation and determined that the payments (totaling approximately 1 million yen) did not qualify as official company expenditures. This case demonstrates that when auditors and other parties carry out their responsibilities, the whistle-blowing system can effectively expose fraudulent acts by corporate management. As a result, Taiyo Yuden is at present making serious efforts to strengthen and conform to its compliance and corporate social responsibility (CSR) standards by adding an outside member to its board of directors and continuing its use of outside auditors.

In 2001, an incident of food poisoning occurred at Snow Brand Milk Products Co., Ltd. After the incident, Snow Brand appointed an outside board member who had severely criticized the company in her previous position as executive director of the National Federation of Consumer Groups. This action was taken in order to change the attitude of the organization concerning safety and compliance.

In order to avoid a repeat of this incident, this new outside board member established a special hotline within the company and went on a tour of the regional

offices and factories, seeking information about violations of compliance. As a result, the number of whistle-blowing cases increased to 13 in 2001, 34 in 2002, and around 20 cases yearly from 2003 to 2006.[9] Management helped employees at each and every factory to voluntarily develop an appreciation of the importance of compliance. This enthusiastic support from management was invaluable in helping Snow Brand to achieve compliance and repair its damaged reputation.

59.6 CONCLUSION

The words *enthusiasm* and *support* are critical when discussing ways to help companies achieve compliance. Management in Japan can face many obstacles when seeking to achieve compliance, including management's own lack of recognition of the importance of compliance. Other obstacles are cultural, such as the Japanese habit of following the crowd and resisting change or Japanese management's tendency to view internal control as a tool that they control rather than a standard they have to conform to. Finally, management must also overcome the more concrete obstacles of assessing their company's internal control components, recognizing existing or potential problems, and developing and implementing effective measures to achieve adequate internal control.

These considerable obstacles can cause management to have a negative attitude toward compliance. But it is critical for management to change this negative attitude and embrace compliance as a positive development for their company's future.

Notes

1. Internal control over financial reporting is defined by the Japanese version of the COSO framework, which is almost the same as the Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the United States. However, the Japanese version of the COSO framework also stresses the utilization of information technology (IT).
2. Mutual shareholding was a traditional Japanese business practice wherein companies that did business with each other held each other's shares as a guarantee of loyalty and as protection against hostile takeovers by other companies.
3. Seibu Railway Co. Ltd. is one of Japan's leading railway operators. It also has a wide range of other business interests, including real estate development, hotel operations, and the Seibu Lions, one of Japan's leading baseball teams.
4. Kanebo, Ltd. was formerly one of Japan's leading manufacturers of cosmetics and fashion products, as well as food products.
5. Livedoor Co., Ltd. is a Tokyo-based Internet company.
6. Article 2 of the new Corporate Law defines a large company as a company with capital of 500 million yen or more, or debt of 20 billion yen or more.
7. Most documents are related to the preparation of flowcharts, narrative documents, or risk control matrix (RCM) documents.
8. Tachibana Securities Co., Ltd., founded in 1953, is a medium-sized securities company.
9. *Nihon Keizai Shinbun*, March 20, 2006.

CHAPTER 60

COMPLIANCE IN MEXICO: TRENDS, BEST PRACTICES, AND CHALLENGES

Pedro Fabiano

60.1 INTRODUCTION

This chapter summarizes current trends, challenges, and opportunities for the implementation of compliance best practices in Mexico. For this purpose, it includes a brief description of the political and economic environment of the country and the local, international, and U.S. standards adopted by Mexico with respect to anticorruption, corporate governance, and anti-money laundering (AML). Compliance statistics from authoritative sources and the resulting challenges and opportunities are also included in the chapter.

60.2 POLITICAL AND ECONOMIC ENVIRONMENT

(a) POLITICAL CONDITIONS. Mexico is the most populous Spanish-speaking country in the world and the second most-populous country in Latin America after Portuguese-speaking Brazil. About 70 percent of the people live in urban areas. Many Mexicans emigrate from rural areas that lack job opportunities to the industrialized urban centers and the developing areas along the United States-Mexico border. According to some estimates, the population of the area around Mexico City is about 18 million, which would make it the largest concentration of population in the western hemisphere. Cities bordering on the United States have undergone sharp rises in population in recent years.

Education is among the Mexican government's highest priorities, and the education budget has continued to grow in recent years. Funding for education increased from 6.9 percent of gross domestic product (GDP) in 2002 to 7.3 percent of GDP in 2005. While efforts to decentralize responsibility for education from the federal to the state level in order to improve accountability are ongoing, the central government still retains significant authority. Although educational performance in Mexico has improved substantially in recent decades, the country still faces several major problems, including providing education to rural and indigenous populations.

Vicente Fox of the National Action Party (PAN) was elected president in July 2000 in what were widely considered the freest and fairest elections in Mexico's history. Fox began his six-year term on December 1, 2000. His victory ended the Institutional Revolutionary Party (PRI)'s 71-year hold on the presidency. President Fox completed his term on December 1, 2006, when Felipe Calderon assumed the presidency.

Numerous electoral reforms implemented since 1989 have progressively opened the Mexican political system, and opposition parties have made historic gains in elections at all levels. At the same time, this opening has left Mexico's political institutions divided. Fox is credited with ending one-party rule and consolidating the opening of Mexico's political system.

Mexico actively participates in several international organizations; it was elected to a seat on the UN Security Council for the period 2002–2003. It is a strong supporter of the United Nations and Organization of American States (OAS) systems and also pursues its interests through a number of ad hoc international bodies. In addition, Mexico does seek to diversify its diplomatic and economic relations, as demonstrated by its accession to the General Agreement on Tariffs and Trade (GATT) in 1986; its joining the Asia-Pacific Economic Cooperation (APEC) forum in 1993; its becoming, in April 1994, the first Latin American member of the Organization for Economic Cooperation and Development (OECD); and its entering the World Trade Organization as a founding member in 1996.

(b) ECONOMIC ENVIRONMENT. Mexico has a free market economy that recently entered the trillion-dollar class ($1.07 trillion for 2005; purchasing power parity (PPP) method/rank in world: 13). It contains a mixture of modern and

outmoded industry and agriculture, increasingly dominated by the private sector. Recent administrations have expanded competition in seaports, railroads, telecommunications, electricity generation, natural gas distribution, and airports. Per capita income is one-fourth that of the United States; income distribution remains highly unequal. Trade with the United States and Canada has tripled since the implementation of the North American Free Trade Agreement (NAFTA) in 1994. Mexico has 12 free trade agreements with over 40 countries, including Guatemala, Honduras, El Salvador, the European Free Trade Area, and Japan, putting more than 90 percent of trade under free trade agreements. The Fox administration was cognizant of the need to upgrade infrastructure, modernize the tax system and labor laws, and allow private investment in the energy sector, but was unable to win the support of the opposition-led Congress. The new government that took office in December 2006 is confronting the same challenges of boosting economic growth, improving Mexico's international competitiveness, and reducing poverty.

Mexico is highly dependent on exports to the United States, which account for almost a quarter of the country's GDP. The result is that the Mexican economy is strongly linked to the U.S. business cycle.

Real GDP grew by 3.0 percent in 2005 and was estimated to grow by 4.5 percent in 2006. Mexico's trade regime is among the most open in the world, with free trade agreements with the United States, Canada, the EU, and many other countries. Since the 1994 devaluation of the peso, successive Mexican governments have improved the country's macroeconomic fundamentals. Inflation and public sector deficits are under control, while the current account balance and public debt profile have improved. As of September 2006, Moody's, Standard & Poor's, and Fitch Ratings had all issued investment-grade ratings for Mexico's sovereign debt.

According to the *OECD Economic Survey of Mexico* released in late 2005, Mexico's economic performance has improved, but not by enough. Since the 1995 financial crisis, Mexico has made progress in terms of economic stability, and the economy is far more open, too. But while poverty has fallen, it remains widespread. Productivity is also low. True, GDP would grow by 4 percent or more for the third year in a row in 2006, the report expected. But although this is better than in several other OECD countries, it is barely enough to keep per capita living standards in Mexico rising at the same rate as the OECD average, let alone close the income gap with the more advanced economies.

The OECD survey also considers that output growth is likely to moderate, reflecting weaker public spending and faltering external demand. Private investment and consumption should remain strong, and GDP growth is projected to reach 3.5 to 4 percent in 2007 and 2008. After turning up in the third quarter of 2006, inflation should come down. With the terms of trade deteriorating, the current account deficit should widen gradually. Monetary policy is expected to ease in early 2007 once inflation has come down. With less growth and lower oil receipts, the environment for fiscal policy will become more difficult, but the fiscal position should not be allowed to weaken. The OECD considers that a

reform is needed to widen the tax base with a view to reducing distortions and financing essential spending programs on a stable basis.

60.3 INTERNATIONAL INITIATIVES AGAINST CORRUPTION

Mexico is a party to the UN Convention Against Corruption, the OECD Convention on Combating Bribery of Foreign Public Officials and the Inter-American Convention Against Corruption.

(a) COMPLIANCE WITH THE OECD CONVENTION. The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, established by the governments of developed countries, is regarded as one of the most important instruments in the fight against corruption.

In 1997, the 29 member nations of the OECD and five nonmember nations adopted the Convention. Signed in December 17, 1997, it sets forth the essential elements of a foreign corrupt practices statute that each signatory country is obligated to enact into law. All signatories to the convention also agreed to implement the Revised Recommendation that includes the elimination of the tax deductibility of bribes.

As of July 2003, all of the Convention's 35 signatories had laws on their books making it a crime to bribe a foreign public official. Mexico is the only Latin American country of the 30 current member states of the OECD.

The convention obligates the parties to criminalize bribery of foreign public officials in the conduct of international business. It proscribes the activities of those who offer, promise, or pay a bribe. For this reason, the antibribery convention is often characterized as a supply-side agreement, as it seeks to affect the conduct of companies in exporting nations.

(b) OECD EVALUATION OF MEXICO. The OECD Convention and the Revised Recommendation are enforced through a program of systematic follow up to monitor and promote their full implementation. This is essentially accomplished through a peer-review process involving two evaluative phases.

Phase 1 involves an examination of the relevant laws and secondary legal sources of each party to determine whether they conform to the requirements under the Convention.

Phase 2 focuses on the application of the laws in practice. It studies the structures put in place to enforce the laws and rules implementing the Convention and to assess their application in practice. Phase 2 broadens the focus of monitoring to encompass more fully the noncriminal law aspects of the Revised Recommendation.

The Mexican legislation was reviewed under Phase 1 in 2000, and the on-site visit for the Phase 2 examination took place in February, 2004. The OECD Evaluation Group concluded that Mexico implemented the Convention through an amendment to the Federal Penal Code (FCC), which establishes the offense of

bribing a foreign public official. Overall, the OECD Evaluation Group considered that the relevant Mexican laws conform generally to the standards under the Convention. However, the Evaluation Group has identified the following issues in the Mexican legislation that require remediation:

- Inconsistent definition of foreign public official
- Exclusion of bribes for the benefit of third parties
- Sufficiency of monetary sanctions
- Effectiveness of criminal liability of legal persons
- Unavailability of sanctions for state-owned and state-controlled companies

60.4 APPLICABLE U.S. LAWS AND REGULATIONS

During the past ten years many of the largest Latin American companies have been on the U.S. markets through the American depositary receipt (ADR) program, while domestic trading has contracted, presenting lower turnover ratios and a very low level of new equity issues.

There is certainly a move toward issuing ADRs, and these seem to improve access to external capital markets. An ADR is equivalent to listing a foreign company's securities on an exchange that protects shareholders, mainly through stricter disclosure requirements. This, in fact, is done by many companies when they list they shares as ADRs in New York.

By the end of 2005, 89 Latin American companies were listed in the New York Stock Exchange (NYSE). The majority of these companies were headquartered in Brazil (35 companies), Chile (18), Mexico (17), and Argentina (12).

According to a recent study published by the Inter American Development Bank (IADB),[1] Mexico is the country with the highest percentage of locally listed firms that have ADRs in the United States. The study shows that close to 38 percent of all Mexican firms listed on the Mexican Stock exchange have some listing in U.S. stock markets. The percentage of firms from Mexico that have ADRs is also among the highest, reaching close to 15 percent.

Importantly, there is no general exemption from the U.S. federal securities laws for foreign private issuers. If their securities are offered or traded in the United States, they need to concern themselves with these laws. The extraterritorial scope of the main U.S. laws related to governance and anticorruption are briefly discussed in the following paragraphs.

(a) FOREIGN CORRUPT PRACTICES ACT OF 1977 AND SARBANES-OXLEY ACT OF 2002. The recent changes to laws and regulations in the United States with respect to governance and fraud have had a considerable impact on foreign private issuers and also on subsidiaries of U.S.-registered entities. A combination of Sarbanes-Oxley (SOX)'s greater focus on internal corporate controls, the increased penalties for Foreign Corrupt Practices Act (FCPA) books and records violations in SOX, and a continued aggressive U.S. government policy to

target international business bribery has resulted in a significant level of FCPA enforcement activity since 2002.

(b) FEDERAL SENTENCING GUIDELINES (FSG). The Federal Sentencing Guidelines for Organizations, issued by the U.S. Sentencing Commission and applicable to criminal violations of all federal statutes such as the FCPA and SOX, require federal courts handing down criminal sanctions to take into account the existence or absence of effective corporate compliance programs. The presence of an effective compliance program can significantly reduce a company's sentence, while the absence of such a program can increase the sentence.

60.5 MEXICAN BEST PRACTICES AND LAWS

(a) CODE OF BEST PRACTICES. The Mexican Committee on Best Corporate Practices was created by pulling forces from the private and the public sector. The Committee was formed by a multidisciplinary group including academics in the area, controlling shareholders of large and small corporations, managers, and representatives of the accounting, finance, and legal professions.

In 1999, this Committee published a Code of Best Practices that included a series of recommendations on what were regarded as good corporate governance practices at the time. The recommendations fell on the four basic areas: (1) disclosure of information related to the administrative structure, objectives, and functioning of the various board committees; (2) the existence of adequate channels for timely disclosure and the existence of good quality of financial information; (3) the adequacy of communication processes between management and board members; and (4) the protection of shareholders' rights, as well as the appropriate disclosure and communication mechanisms with them.

The Mexican Code of Best Practices was the first in Latin America, and one of the first in the world, as it came before the U.S. corporate governance scandals. At the time, only the United Kingdom and a few other countries had implemented such an approach to try to foster more transparency in the market and a mechanism that facilitated the transmission of information to investors.

In January 2001, a Mexican commission of business leaders, with the support of the Mexican National Banking and Securities Commission (the CNBV), endorsed the Code of Best Corporate Practices for publicly traded Mexican companies, recommending certain actions with respect to various areas of corporate governance. The Mexican Securities Market Law was amended effective June 2001 to require that all publicly traded Mexican companies have an audit committee. In March 2003, the CNBV codified certain provisions of the Code of Best Corporate Practices, requiring among other things, increased responsibilities for audit committees. While compliance with the Code of Best Corporate Practices is voluntary, the CNBV requires companies listed on the Mexican Stock Exchange to file a report, on a yearly basis, regarding their compliance with the Code of Best Corporate Practices.

Starting with fiscal year 2000, all publicly traded firms on the Mexican Stock Exchange must state in their annual report to the shareholders which rules of the code they follow, and which they do not. They may state why they do not follow the rules they have elected not to follow, and describe any alternate mechanisms they may have for the protection of investors. All firms with publicly trading securities, both equity and debt, have to disclose the information.

The list of corporate governance practices that was created at the time consists of mandatory answers to 55 questions. Although firms are not required to meet the recommendations of the code, the fact that all firms with publicly traded securities have to disclose this has been useful to investors.

(b) COMPLIANCE WITH MEXICAN CODE OF BEST PRACTICES. In July 2006, the Inter American Development Bank published a research study[2] that measured compliance with Mexican Code of Best Practices. The study shows the principal descriptive statistics of the corporate governance (CG) index for the 150 firms in the sample. The CG index is the average of the indexes for the two years (2003 and 2004) for which company data has been disaggregated. The main conclusions of the study are:

- The mean company in Mexico met 78.4 percent of all the recommendations in the code.
- The best firm showed a 98.2 percent rate of compliance, while the worst firm met less than 30 percent of the code's recommendations.
- In 2004, close to 90 firms out of the 150 in the sample met more than 80 percent of the code's recommendations. Another 35 firms met between 70 and 80 percent of the code, bringing the cumulative percentage of firms above 70 percent compliance to 83 percent of the sample.
- Compliance has increased over time. In 2000, the first year of the code, the mean firm followed 64 percent of the principles while the following year the number jumped to 70 percent.
- The period 2002–2004 saw smaller increases leaving the total compliance close to 77 percent at the end of the period. Compliance increased only 1 percent from 2003 to 2004, suggesting a slowdown in change of corporate practices.

(c) NEW MEXICAN SECURITIES MARKET LAW. In December 2005, a new Mexican Securities Market Law was enacted with a focus on increasing its adherence to international standards, including increased protections for minority shareholders. Included in the new law is the requirement that all publicly traded Mexican companies have a corporate practices committee. The new law will introduce significant changes to the current regime in which issuers operate, including:

- The establishment of the *sociedad anónima bursátil*, a separate corporate form of organization for issuers with stock registered with the CNBV and

listed on the Mexican Stock Exchange, which provides for a new set of corporate governance requirements.

- The redefinition of the functions and structure of the board of directors, including (1) increasing the number of members of the board of directors (up to 21, with independent members comprising at least 25 percent) and (2) requiring that the status of members of the board of directors as independent be determined by the shareholders' meeting, subject to the CNBV's authority to challenge such determination.
- The application of a legal framework to the chief executive officer and executive officers entrusted with the day-to-day management of the issuer.
- The adoption of a clear definition of fiduciary duties, including but not limited to the duty of care and the duty of loyalty, for members of the board of directors and its secretary, the chief executive officer and other executive officers.
- The increase in liability for members of the board of directors and its secretary with respect to the operations and performance of the issuer, including (1) payment of damages and losses resulting from the breach of their duty of care or loyalty and (2) criminal penalties from 1 to 12 years of imprisonment for certain illegal acts involving willful misconduct. Civil actions under (1) may be brought by the issuer or by shareholders that represent 5 percent or more of the capital stock of the issuer; and criminal actions under (2) may only be brought by the Mexican Ministry of Finance, after consultation with the CNBV.
- The elimination of the requirement that the issuer have a statutory auditor and the delegation of specific obligations of corporate governance and oversight to the audit committee, the corporate practices committee and the external auditors.
- The requirement that all the members of the audit and corporate practices committees be independent as such term is defined under the new law, except with respect to the corporate practices committee in the case of issuers like us that have a controlling shareholder.
- The enhancement of the functions and responsibilities of the audit committee, including (1) the evaluation of the performance of the external auditors; (2) the review and discussion of the financial statements of the issuer and the conveyance to the board of directors of the committee's recommendations regarding the approval of such financial statements; (3) the surveillance of internal controls and internal audit procedures of the issuer; (4) the reception and analysis of recommendations and observations regarding the committee's functions by the shareholders, members of the board of directors, and senior management, and the authority to act upon such recommendations and observations; (5) the authority to call a shareholders' meeting and to contribute to the meeting's agenda; and

(6) the oversight of the execution of resolutions enacted at meetings of shareholders or the board of directors.

- The requirement that the shareholders' meeting approve all transactions that represent 20 percent or more of the consolidated assets of the issuer within a given fiscal year.
- The inclusion of a new set of rules requiring an issuer to obtain prior authorization from the CNBV to effect public offerings of securities and tender offers.

(d) MAJOR CHALLENGES IN ANTICORRUPTION AND GOVERNANCE. The World Bank research conducted on governance indicators ("Governance Matters V," 2006) supports the fact that realistic improvement in a nation's rule of law or control of corruption could result in a significant percent increase in per capita incomes in the long term. Governance is broadly defined by the World Bank as *the traditions and institutions by which authority in a country is exercised*. The individual measures of governance perceptions were assigned to six categories capturing key dimensions of governance:

Voice and Accountability: the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and free media.

Political Stability and Absence of Violence: perceptions of the likelihood that the government will not be destabilized or overthrown by unconstitutional or violent means, including domestic violence and terrorism.

Government Effectiveness: the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies.

Regulatory Quality: the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development.

Rule of Law: the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, the police, and the courts, as well as the likelihood of crime and violence.

Control of Corruption: the extent to which public power is exercised for private gain, including both petty and grand forms of corruption, as well as capture of the state by elites and private interests.

Exhibit 60.1 includes the indicators for the six World Bank governance categories. Compared with the OECD average, Mexico shows very low scores for all of the six governance categories. Exhibits 60.2 and 60.3 reveal that, in general, Mexico shares poor law enforcement and weak control of corruption with most of the countries in Latin America and ranks below Chile, Uruguay, and Brazil, among others.

2006 Governance Indicator	Latin America Regional Average Percentile (1–100)*	OECD Regional Average Percentile (1–100)*	Mexico Percentile (1–100)*
Voice and Accountability	51.6	90.6	52.4
Political Stability/No Violence	37.7	76.4	32.7
Government Effectiveness	43.2	90.0	60.7
Regulatory Quality	45.4	89.6	63.4
Rule of Law	35.4	90.0	40.5
Control of Corruption	42.0	90.0	46.6

*Higher values imply better Governance ratings. Percentile rank indicates the percentage of regions that rate below the selected region.
Source: Kaufmann, Daniel, Aart Kraay, and Massimo Mastruzi ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 60.1 WORLD BANK GOVERNANCE RANKINGS: SIX ELEMENTS FOR MEXICO, LATIN AMERICA, AND OECD

Country/Regions	2006 Country Percentile (1–100)*	2006 Latin America Regional Average Percentile (1–100)*	2006 OECD Regional Average Percentile (1–100)*
Argentina	35.7	35.4	89.6
Bolivia	20.5	35.4	89.6
Brazil	41.4	35.4	89.6
Chile	87.6	35.4	89.6
Colombia	29.5	35.4	89.6
Costa Rica	64.8	35.4	89.6
Dominican Republic	39.5	35.4	89.6
Ecuador	16.2	35.4	89.6
El Salvador	37.6	35.4	89.6
Guatemala	14.3	35.4	89.6
Honduras	21.4	35.4	89.6
Mexico	40.5	35.4	89.6
Nicaragua	25.7	35.4	89.6
Panama	51.4	35.4	89.6
Paraguay	18.1	35.4	89.6
Peru	26.2	35.4	89.6
Uruguay	61.0	35.4	89.6
Venezuela	5.7	35.4	89.6

*Higher values imply better Governance ratings. Percentile rank indicates the percentage of regions that rate below the selected region.
Source: Kaufmann, Daniel, Aart Kraay, and Massimo Mastruzi ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 60.2 WORLD BANK GOVERNANCE RANKINGS: RULE OF LAW FOR LATIN AMERICAN AND OECD AVERAGES

Country/Region	2006 Country Percentile (1−100)*	2006 Latin America Regional Average Percentile (1−100)*	2006 OECD Regional Average Percentile (1−100)*
Argentina	40.8	42.0	90.5
Bolivia	31.1	42.0	90.5
Brazil	47.1	42.0	90.5
Chile	89.8	42.0	90.5
Colombia	51.9	42.0	90.5
Costa Rica	67.0	42.0	90.5
Dominican Republic	34.0	42.0	90.5
Ecuador	24.8	42.0	90.5
El Salvador	53.9	42.0	90.5
Guatemala	26.7	42.0	90.5
Honduras	22.3	42.0	90.5
Mexico	46.6	42.0	90.5
Nicaragua	23.8	42.0	90.5
Panama	49.5	42.0	90.5
Paraguay	13.6	42.0	90.5
Peru	45.1	42.0	90.5
Uruguay	75.2	42.0	90.5
Venezuela	12.6	42.0	90.5

*Higher values imply better Governance ratings. Percentile rank indicates the percentage of countries worldwide that rate below the selected country.
Source: Kaufmann, Daniel, Aart Kraay, and Massimo Mastruzi ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 60.3 WORLD BANK GOVERNANCE RANKINGS: CONTROL OF CORRUPTION FOR LATIN AMERICAN COUNTRIES AND OECD AVERAGES

60.6 ANTI-MONEY LAUNDERING COMPLIANCE

(a) INTERNATIONAL ORGANIZATIONS. Mexico is member of the Financial Action Task Force Against Money Laundering (FATF), and participates in the Caribbean Financial Action Task Force as a cooperating and supporting nation and in the South American Financial Action Task Force as an observer member. Mexico is a member of the Egmont Group and the Organization of American States (OAS) agency Inter-American commission for the Control of the Abuse of Drugs (CICAD) Experts Group to Control Money Laundering. In addition, Mexico is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Terrorism.

(b) MONEY LAUNDERING IN THE MEXICAN FINANCIAL SYSTEM[3]. Currently, there are 29 commercial banks and 71 foreign financial representative offices operating in Mexico, with seven commercial banks representing 89 percent of total assets in the banking sector. Commercial banks, foreign exchange companies, and general commercial establishments are allowed to offer money exchange services. Mexico has 87 insurance companies, 13 bonding institutions, 178 credit unions, and 24 money exchange houses. The size of the underground economy is unknown, although it is estimated to account for anywhere between 20 and 40 percent of the gross domestic product in Mexico. However, the informal economy is considered to be much less of a problem overall than that of the narcotics-driven segments of the economy. Beginning in 2005, permits were issued for casinos to operate in Mexico. Gambling is also legally allowed through national lotteries, horse races, and sport pools. Casinos and offshore banks are currently not subject to anti-money laundering reporting requirements.

Since 2000, Mexicans have received an estimated $52 billion in remittances, and conservative estimates indicate that this amount will increase to over $80 billion by the end of 2006. Remittances from the United States to Mexico reached a record high $20 billion in 2005. Although nonbank companies continue to dominate the market for remittances, many U.S. banks have teamed up with their Mexican counterparts to develop systems to simplify and expedite the transfer of money. These measures include wider acceptance by U.S. banks of the *matricula* consular, an identification card issued by Mexican consular offices to Mexican citizens residing in the United States that has been criticized, based on security issues. In some cases, neither the sender nor the recipient of a remittance is required to open a bank account in the United States or Mexico, but must simply provide the *matricula* consular as identification and pay a flat fee. Although these systems have been designed to make the transfer of money faster and less expensive for the customers, the rapid movement of such vast sums of money by persons of questionable identity leaves the new money transfer systems open to potential money laundering and exploitation by organized crime groups.

The illicit drug trade continues to be the principal source of funds laundered through the Mexican financial system. Mexico is a major drug producing and drug-transit country. Mexico also serves as one of the major conduits for proceeds from illegal drug sales leaving the United States. Other crimes, including corruption, kidnapping, firearms trafficking, and immigrant trafficking are also major sources of illegal proceeds. The smuggling of bulk shipments of U.S. currency into Mexico and the movement of the cash back into the United States via couriers, armored vehicles, and wire transfers, remain favored methods for laundering drug proceeds. Mexico's financial institutions are vulnerable to currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States.

According to U.S. law enforcement officials, Mexico remains one of the most challenging money laundering jurisdictions for the United States, especially with regard to the investigation of money laundering activities involving the cross-border smuggling of bulk currency from drug transactions.

While Mexico has taken a number of steps to improve its anti-money laundering (AML) system, significant amounts of narcotics-related proceeds are still smuggled across the border. In addition, such proceeds can still be introduced into the financial system through Mexican banks or bureaus of exchange, or repatriated across the border without record of the true owner of the funds. Corruption is also a concern. In recent years, various Mexican officials, including former officials from the Mexico City government, have come under investigation for alleged money-laundering activities.

In 2005, U.S. authorities observed a significant increase in the number of complex money-laundering investigations by the Financial Crimes Unit of the Office of the Deputy Attorney General Against Organized Crimes (SIEDO), including cases coordinated with U.S. officials. The U.S. Treasury Department's Office of Foreign Asset Control (OFAC) announced in January 2005 the designation of 39 "Tier II" targets involved in significant narcotics trafficking. Some of these designations centered on foreign exchange centers, which fall under the supervision of the Secretariat of Finance and Public Credit (Hacienda). The designation of these companies, which are associated with the previously designated Arellano Felix drug trafficking organization, under the Foreign Narcotics Kingpin Designation Act, resulted from cooperation among OFAC, other U.S. government entities, and SIEDO. These designations allowed U.S. and Mexican authorities to seek the freezing of assets of Mexican drug cartels, hindering their ability to take advantage of the U.S. and Mexican financial systems.

(c) ANTI-MONEY LAUNDERING LAWS AND REGULATIONS. The Government of Mexico continues efforts to implement an AML program according to international standards such as those of the Financial Action Task Force (FATF), which Mexico joined in June 2000. Money laundering related to all serious crimes were criminalized in 1996 under Article 400b of the Federal Penal Code, and is punishable by imprisonment of five to fifteen years and a fine. Penalties are increased when a government official in charge of the prevention, investigation, or prosecution of money laundering commits the offense.

In 1997, the Government of Mexico established a financial intelligence unit (UIF).The UIF is responsible for receiving, analyzing, and disseminating financial reports from a wide range of obligated entities. The UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials.

Regulations have been implemented for banks and other financial institutions (mutual savings companies, insurance companies, financial advisers, stock markets, and credit institutions), as well as exchange houses, and money remittance businesses to know and identify customers and maintain records of

transactions. These entities must report suspicious transactions, transactions over $10,000, and transactions involving employees of financial institutions who engage in unusual activity to the UIF. Financial institutions with a reporting obligation now require occasional customers performing transactions equivalent to or exceeding $3,000 in value to be identified, so the transactions can be aggregated daily to prevent circumvention of the requirements to file cash transaction reports (CTR) and suspicious transaction reports (STR). Financial institutions also have implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers. Real estate brokerages, attorney, notaries, accountants, and dealers in precious metals and stones are required under a November 2005 provision of the tax law to report all transactions exceeding $10,000 to the UIF, via the Tax Administration Service. In 2005, the FIU received approximately 4,800,000 CTRs and 57,700 STRs from obligated entities.

In December 2000, Mexico amended its Customs Law to reduce the threshold for reporting inbound cross-border transportation of currency or monetary instruments from $20,000 to $10,000. At the same time, it established a requirement for the reporting of outbound cross-border transportation of currency or monetary instruments of $10,000 or more. These reports are also received by the UIF. Efforts are ongoing to compare the declarations filed in Mexico with those filed in the United States to determine compliance with this reporting requirement. However, Mexico's reporting requirements include a wider range of monetary instruments (e.g., bank drafts) than those of the United States.

(d) FATF EVALUATION OF MEXICO. In September 2003, Mexico underwent its second mutual evaluation by the FATF, and the findings of the evaluation team were accepted at the FATF plenary meetings in June 2004. The evaluation team Money Laundering and Financial Crimes found that Mexico had made progress since the first mutual evaluation by removing specific exemptions to customer identification obligations, implementing online reporting forms and a new automated transmission process for reporting transactions to the UIF, and slightly reducing the delay in reporting transactions overall. The government of Mexico also developed an overall anti-money laundering strategy and plan.

However, the FATF evaluation team also identified a number of deficiencies in the system. Mexico does not have a separate offense of terrorist financing. Bank and trust secrecy were considered impediments to many aspects of Mexico's anti-money laundering/counterterrorist financing system (AML/CTF), particularly for law enforcement and prosecutorial and judicial authorities during investigations and prosecutions. As a result of these deficiencies, the Government of Mexico must update the FATF on its progress, which it did at the June and October 2005 plenary meetings of the FATF. While Mexico has not yet criminalized terrorist financing, it has made improvements to its bank secrecy laws.

Amendments to the Banking Law that were approved in April 2005 now allow specific government entities, such as the Profit Review Group (PGR) and the state attorney generals, to receive records directly from banks without prior approval from the National Banking and Securities Commission (CNBV). Previously, all requests to lift bank secrecy had to be approved by the CNBV. Financial institutions must respond to these requests within three days.

In November 2003, the Senate passed a bill amending the Federal Penal Code that would link terrorist financing to money laundering. However, little progress was made with regard to the passage of this bill by the Congress. In 2005, the draft legislation was resubmitted as two separate draft laws: one to criminalize the financing of terrorism and one to address outstanding international cooperation issues.

This legislation, once passed, is intended to bring Mexico into compliance with international standards. The proposed amendments would also create two new crimes: conspiracy to launder assets and international terrorism (when committed in Mexico to inflict damage on a foreign state). The draft legislation is currently under consideration in the Senate.

(e) COOPERATION WITH U.S. AUTHORITIES. Although Mexico does not have a specific crime criminalizing the financing of terrorism because terrorism is declared to be a serious crime, money laundering associated with terrorism is punishable under the existing Penal Code. The government of Mexico has responded to U.S. government efforts to identify and block terrorist-related funds, and, although no assets were frozen, it continues to monitor suspicious financial transactions.

Although the United States and Mexico both have forfeiture laws and provisions for seizing assets abroad derived from criminal activity, U.S. government requests to Mexico for the seizure, forfeiture, and repatriation of criminal assets have not met with success, as Mexican authorities have difficulties with assets seized for forfeiture in Mexico if these assets are not clearly linked to narcotics. Most assets seized during law enforcement operations go to the Service for the Management and Transfer of Assets (SAE), a semiautonomous branch of the Hacienda established in late 2002. Although Mexican officials have made significant progress in modernizing their approach to asset seizure, actual asset forfeiture remains a challenge. In two significant U.S. cases involving fraud, authorities seized real property and money generated from the crime. Although authorities gained forfeiture of the property in the United States, counterparts in Mexico did not carry out such orders in Mexico, nor have they returned related assets to the United States for forfeiture.

Mexico has developed a broad network of bilateral agreements with the United States, and regularly meets in bilateral law enforcement working groups with the United States. The U.S.-Mexico Mutual Legal Assistance Treaty entered into force in 1991. The Mexican and U.S. governments continue to implement

other bilateral treaties and agreements for cooperation in law enforcement issues, including the Financial Information Exchange Agreement (FIEA) and the memorandum of understanding (MOU) for the exchange of information on the Cross-border Movement of Currency and Monetary Instruments. In February 2005, the UIF and the U.S. financial intelligence unit, FinCEN, signed an MOU further detailing the procedures for information exchange. The U.S. Customs Service and Mexico City entrepreneurs have established a Business Anti-Smuggling Coalition, including a financial BASC chapter created to deter money laundering, which remained active in 2005.

60.7 CONCLUDING REMARKS

Mexico has demonstrated its leadership in the development of best practices that encourage transparency and improve investor protection. The creation and further implementation of the first Code of Corporate Governance in Latin America, and the recent success in passing a new Securities Law are measures aimed to substantially increase the level of disclosure and to improve corporate governance requirements for listed firms.

In the area of AML/CTF, the most recent FATF evaluation found that Mexico had made significant progress since the first mutual evaluation. In spite of this progress, the main challenges in this area include: a closer monitoring of the remittance systems for possible exploitation by criminal groups, the enactment of the proposed legislation to criminalize the financing of terrorism and the effectiveness in prosecuting and convicting money launderers.

However, legal rules are only one element of the investor protection and AML/CTF systems. The enforcement of these rules may be equally or even more important. The major opportunity for Mexico is heavily dependent on its ability to resolve the law enforcement and control of corruption issues, which will allow the country to enhance the effectiveness of the recent reforms in laws and regulations.

Notes

1. Alberto Chong and Florencio López-de-Silanes, "Corporate Governance and Firm Value in Mexico" (IADB Research Department Working Paper 564, July 2006).
2. Ibid.
3. International Narcotics Control Strategy Report 2006 (INCSR), published by the United States Department of State-Bureau for International Narcotics and Law Enforcement Affairs.

CHAPTER 61

CORPORATE GOVERNANCE IN RUSSIA

Anthony Tarantino, PhD

61.1 INTRODUCTION

The image of Russia around corporate governance is one of excitement on the one hand as the investors enjoy a booming market, and concern on the other hand as the government uses strong-arm tactics against dissidents, and its energy resources as a political weapon. One constituency has a strikingly positive take on Russia and its president, Vladimir Putin. Russia's stock market has enjoyed a major rally over the seven years of Putin's administration. In 2000 publicly traded stocks were valued at $74 billion. They now exceed $1 trillion in value. The Russian Trading System (RTS) Stock Exchange index has risen 71 percent in 2006 alone, and averaged over 50 percent growth over the past four years.[1]

The critics of Putin may concede that Russia has made major progress in bringing capitalism to the former Soviet Union, but challenge his methods. Russia has enjoyed political and economic stability under Putin. A major criticism to his capitalism advancement is the creation of state-run enterprises, which we discuss later in the chapter. Oil is the primary reason for the economic stability, with Russia as the world's largest oil exporter, behind only Saudi Arabia. But Putin has done much to turn around a nation that eight years ago defaulted on its debt. Putin's supporters can also note that Russia has one of the world's largest foreign-exchange reserves and is running large budget surpluses, including a $89 billion reserve.[2]

Some investors and analysts have expressed concerns that human rights will need to improve over the long term in order for Russia to sustain its high growth rates. The murder of former KGB agent Alexander Litvinenko remains unsolved and made worldwide headlines with his deathbed accusation that Putin was responsible for his poisoning. Also making headlines has been a series of acts against other former officials and journalists who have criticized the Russian government. These acts have increased concerns that Russia is losing ground in embracing the rule of law and the control of corruption.

It is true that the makeup of Russia's ruling elite has changed over the past six years with the ascension of several former security service officers to top administrative posts under President Putin. In the past few years, most of the top ministers, half of the members of the Russian security council, and 70 percent of all senior regional officials in Russia were former members of the security services.[3]

This phenomenon has also occurred in other former Soviet bloc nations, and should not come as any great surprise given the vital importance intelligence services have played during the cold war. The first U.S. President Bush had been head of the Central Intelligence Agency, and Robert Gates, the new Secretary of Defense, charged with getting the United States out of the mess in Iraq, is also a former CIA chief. Intelligence agencies have typically represented an elite and intellectual class who know how to make things happen one way or the other—following or bending rules as required. The argument follows: Who better to move Russia forward posthaste in a nation that has not traditionally possessed the business, legal, and governance skills available in the West? The argument continues that this is a transitional mode until Russia has trained a generation of business, legal, and financial leaders comfortable in Western market and governance practices. The counterargument is that former intelligence officers trained during the cold war are not likely to embrace Western concepts of governance, ethics, or morality.

The Yukos scandal has created one of the most controversial areas for President Putin in recent years. Yukos is Russia's second largest oil company and was headed by Russia's richest man, Mikahail Khodorkovsky. He was prosecuted for fraud and tax evasion. The controversy arose over the reason for his imprisonment, with government critics charging it was over his support of government opponents, while the government responded that it was over his massive corruption in attempting to force the Duma to modify tax laws in his favor.

Putin's press media critics such as the Committee to Project Journalists charge that much of the press media is now under at least indirect control or pressure throught the use of hostile takeover and punitive tax audits. They also claim that all three major television networks are controlled by government loyalists.[4]

Putin's critics charge that public administration in Russia suffers from poor quality and a lack of government reform efforts—limited to reorganization and role definitions. These critics also charge that the government has focused much of its attention on amassing assets in strategic sectors of the economy which has, as a by-product, increased corruption and reduced transparency. Some of this may be the result of a residue from the Soviet-era bureaucracy and a powerful patronage system.

Russia's decade-long efforts to join the World Trade Organization (WTO) are close to coming to fruition. Russia will face changes similar to those faced by China, admitted in 2001. Intellectual property rights, free press, nationalization of energy industries, and the control of corruption will all be issues of interest to the WTO and the international community.

In spite of concerns about corporate governance, Russia continues to attract foreign investors. In the first half of 2006, Russia attracted $23.4 billion of foreign investment, an increase of 41.9 percent over the first half of 2005. The attraction is clear to see—a fast growing economy. With an average GDP growth rate of about 6 percent over several years, it lags behind only China and India and is well above EU and U.S. rates. Investors also point to its economic stability, solvency, strong national currency, and AT Kearney's sixth-place ranking in its 2005 confidence index as positive factors. The primary problems investors report are around the bureaucratic system, legal system, corruption, and the lack of quality corporate management.[5]

61.2 SOVEREIGN DEMOCRACY

The Putin administration's political philosophy has been described as sovereign democracy (Суверенная демократии), and it is gaining acceptance and helping unify support within Russia. The sovereign democracy takes a populist approach to government and downplays reliance on foreign models to drive reform. If this philosophy takes root, it will have a direct and major impact on efforts to improve corporate governance, the rule of law, control over corruption, and freedom of information.

It is important to put all this in perspective and realize how far Russia has come since the days of the Soviet Union under Leonid Brezhnev. Yes, Russia is very different from Western governments with what the *Economist* describes as its "Gazpromistan, or Kremlin Inc.—a hybrid of authoritarian bureaucracy and capitalism which turns wealth into power, and then power back into wealth—at home and abroad."[6]

61.3 STATE-OWNED ENTERPRISES

One manifestation of the wealth to power process is the nationalization of Russian natural resource sectors. The Russian company Rusal, through mergers and acquisitions, is now the largest aluminum company in the world with a new name of Russian Aluminum. Gazprom is a state-owned natural-gas monopoly and has a market value of $250 billion, nearly the size of ExxonMobil. Gazprom has become a dominant factor and concern in EU energy policies.[7]

The Organization for Economic Cooperation and Development (OECD) tracks the progress of its member and affiliated states in improving corporate governance. In its 2006 report, the OECD criticized Russia for moving in the wrong direction by nationalizing key industries, such as energy and metals. The concern is that this may increase corruption, which already is a major issue in Russia.

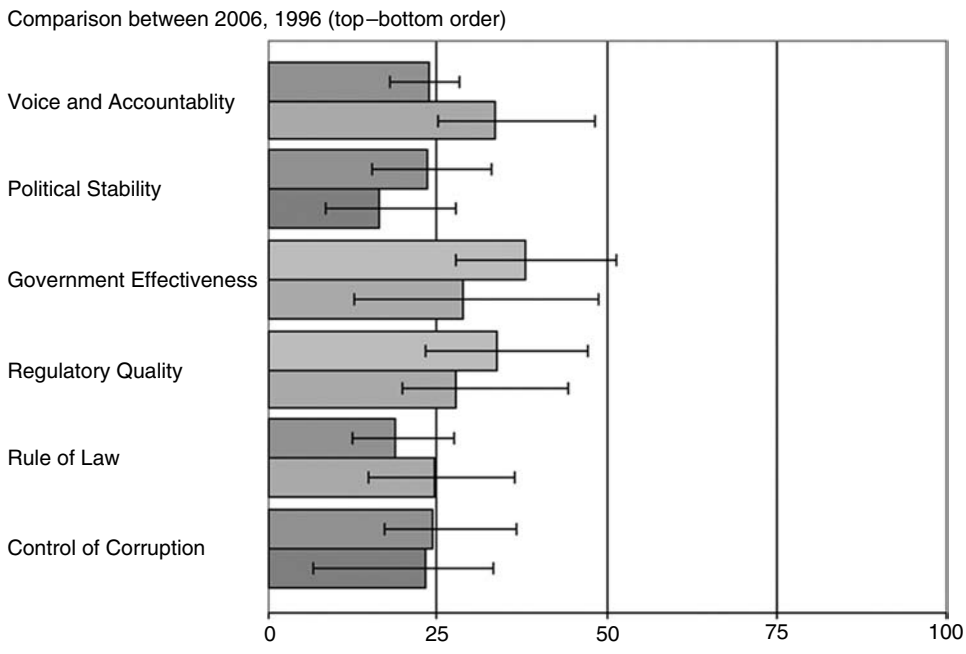
Beyond corruption, the failure of nationalized industries in several countries over the past 50 years makes this move problematic at best. Nationalized

industries are typically inefficient, and burdened with excessive bureaucracy and corruption. China's nationalized industries continue to struggle, while its private enterprises are among the most competitive in the world. Nationalized energy industries in Mexico and Venezuela are typically viewed as among the most corrupt and inefficient enterprises.

So it is hard to find a successful role model for Russia's action beyond exerting political power. The OECD fears nationalization may slow its fast growing economy, and that the state's interference in company operations can cripple and distort their development. The Russians do not appear to be intimidated by these foreign concerns, feeling the need to attract foreign investment is not as important as in the past.

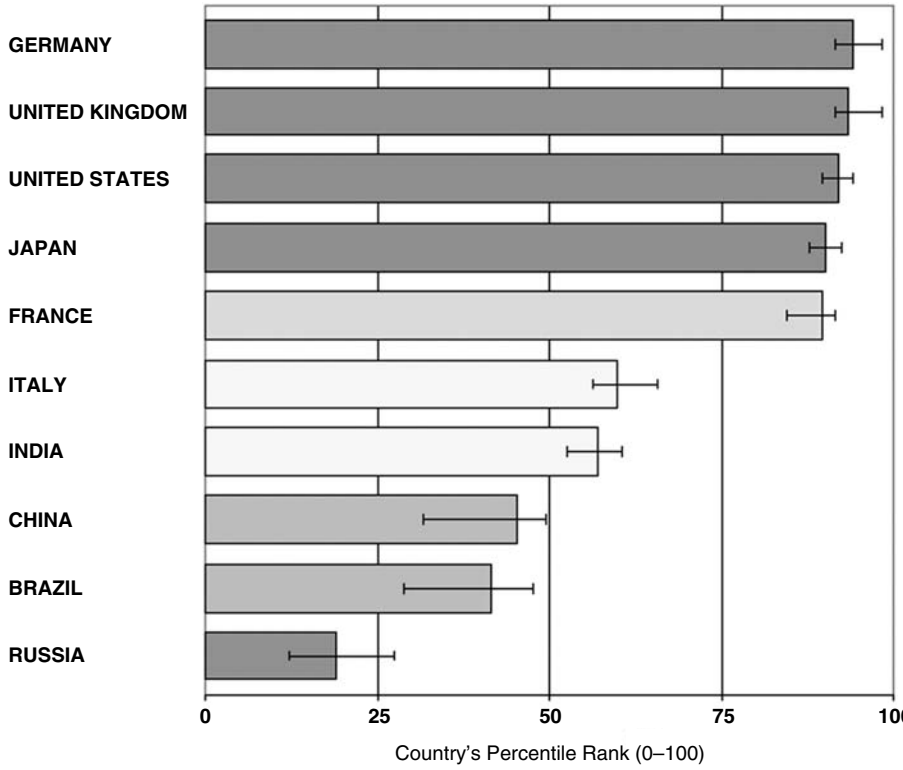
61.4 WORLD BANK GOVERNANCE METRICS

The World Bank publishes country-to-country and year-to-year comparisons of six areas of governance. These metrics demonstrate that Russia has a long way to go to reach Western standards of governance. The 1996 to 2006 ratings



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 61.1 WORLD BANK GOVERNANCE RANKINGS: SIX ELEMENTS FOR RUSSIA 2006 AND 1996 (TOP-TO-BOTTOM ORDER)



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 61.2 WORLD BANK GOVERNANCE RANKINGS: RULE OF LAW FOR RUSSIA AND MAJOR GDP COUNTRIES

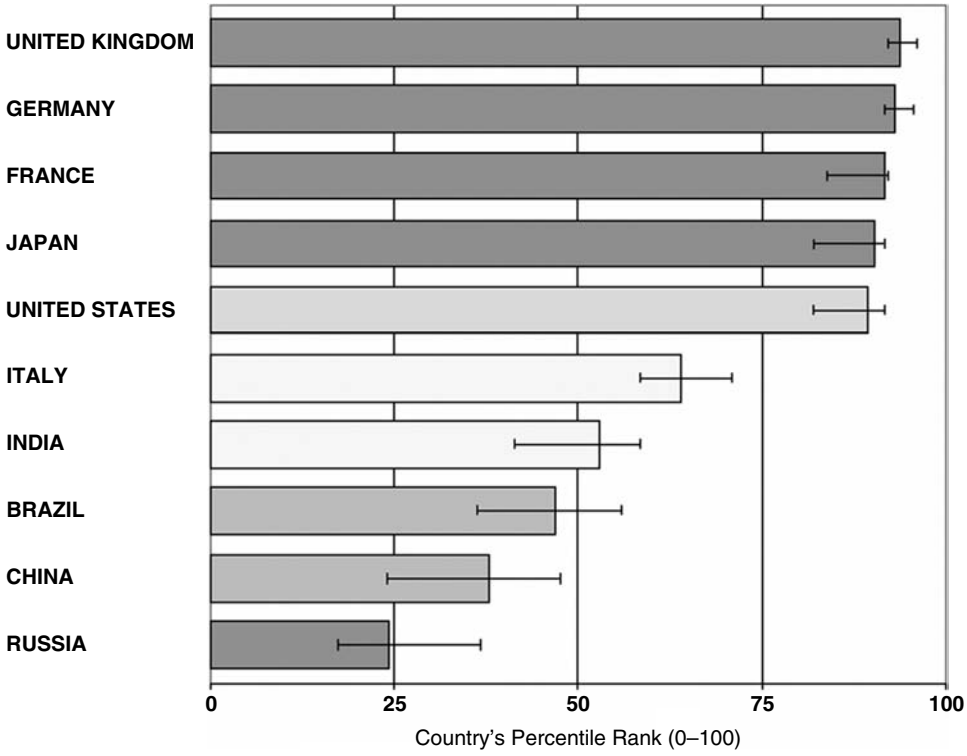
show improvements in government effectiveness and regulatory quality, minimal change in control of corruption, rule of law, political stability/no violence, and a major decline in voice and accountability. (See Exhibits 61.1 to 61.5.)

61.5 CURRENT STATE OF CORPORATE GOVERNANCE

According to the U.S. Commerce Department's International Trade Administration (ITA), the current state of Russian corporate governance may be characterized in the following ways:[8]

CONCENTRATED OWNERSHIP

- "Most Russian companies are controlled by a single controlling shareholder or small group of shareholders. This holds true not only for the natural resource sector, but communications, metallurgy, and forestry as well.
- Concentrated ownership structure can often result in minority shareholder abuses.



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 61.3 WORLD BANK GOVERNANCE RANKINGS: CONTROL OF CORRUPTION FOR RUSSIA AND MAJOR GDP COUNTRIES

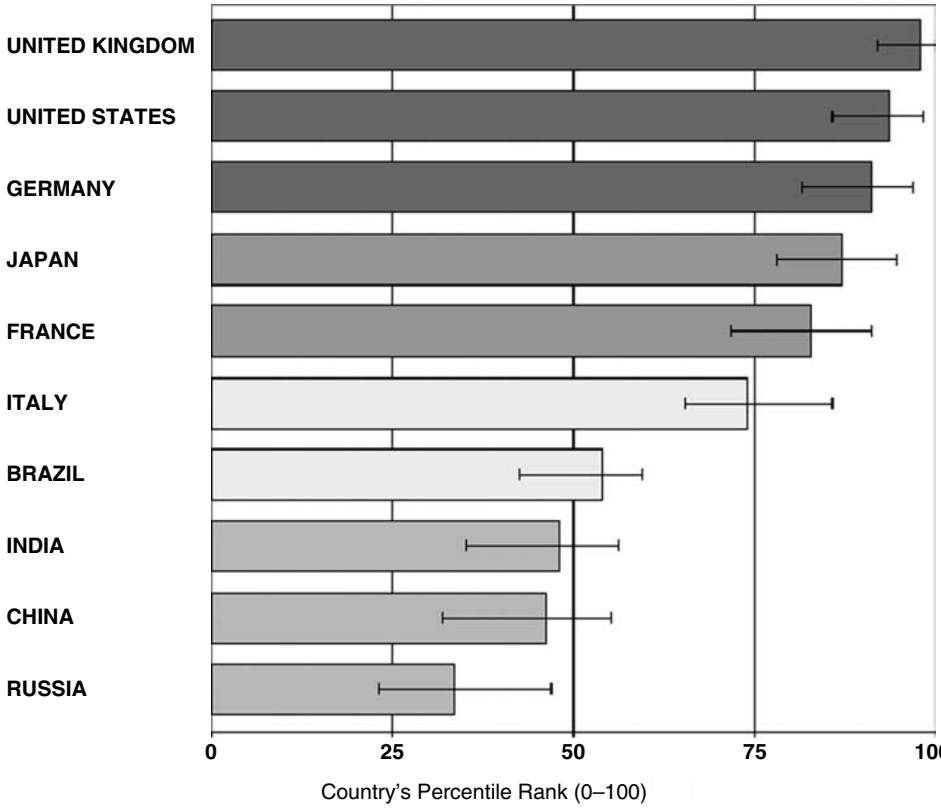
- Insider dominance and the weak protection of external stakeholders has hurt the development of Russian capital markets."

LITTLE SEPARATION OF OWNERSHIP AND CONTROL

- "Many controlling shareholders also act as the company's general director and sit on the supervisory board.
- Companies that do separate ownership and control often do so only on paper.
- Such companies often suffer from weak accountability and control structures, abusive related party transactions, and poor information disclosure."

UNWIELDY HOLDING STRUCTURES

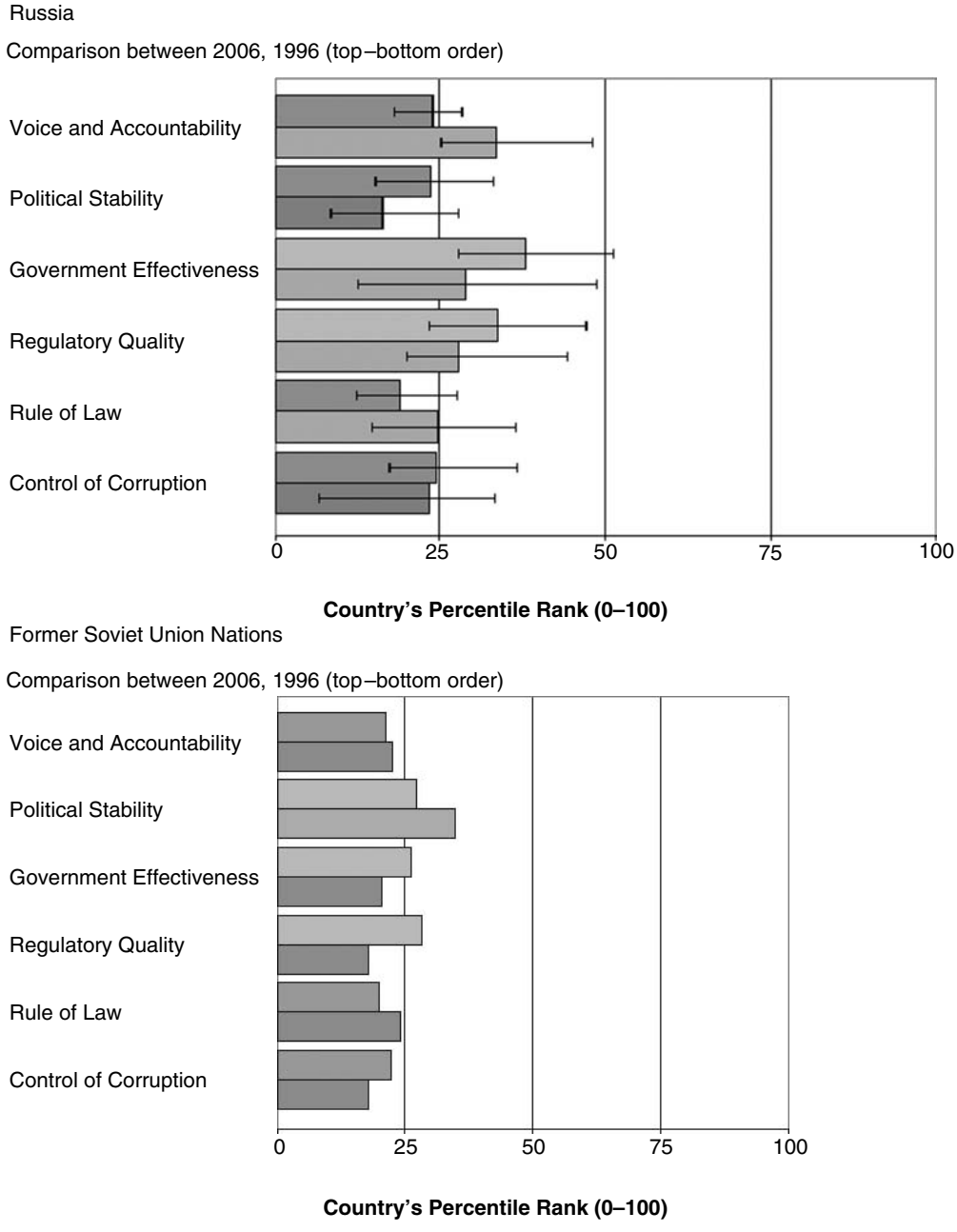
- "Major business groups in the form of holding companies control companies in most industries.



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 61.4 WORLD BANK GOVERNANCE RANKINGS: REGULATORY QUALITY FOR RUSSIA AND THE MAJOR GDP COUNTRIES

- While holding structures can serve legitimate purposes, complex business structures, cross-shareholdings, pyramid structures, and other arrangements to create opaque ownership structures can make the company difficult to understand for shareholders and investors.
- Such structures are often used to expropriate and circumvent the rights of individual shareholders.
- Poor consolidated accounting, or even the absence thereof, is a further corporate governance issue that has yet to be tackled.
- Many of these holding structures are currently being reorganized for various reasons. Some controlling shareholders have discovered a desire to build and run proper businesses—based on good corporate governance—thus leaving a positive legacy behind. Others seek to properly transfer their businesses to the next generation or sell their stakes to outside investors."



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 61.5 WORLD BANK GOVERANCE RANKINGS: REGULATORY QUALITY FOR RUSSIA (UPPER CHART) AND FORMER SOVIET UNION NATIONS (LOWER CHART)

Inexperienced and Inadequate Supervisory Boards

- "The concept of supervisory bodies was only introduced with Russia's transition to a market economy. Such a supervisory structure did not exist in state-owned enterprises during the Soviet Union.
- General directors often seek to bypass this supervisory structure, seeking direct contact with the controlling shareholder (inasmuch as they are not one and the same person).
- The role of supervisory boards often remains unclear, with some taking on authorities that belong to the executive management and others becoming actively involved in the company's day-to-day management.
- Strong, vigilant, and independent supervisory boards remain a rarity."

Legal and Regulatory Framework

- "Russia's legal and regulatory framework for corporate governance has improved dramatically but remains nascent.
- The first comprehensive piece of legislation was approved in late 1995 when the Law on Joint Stock Companies was adopted. By that time, however, many companies had already been created, most in the wake of the first phase of privatization, and a proper corporate governance structure to guide companies was largely absent.
- Today, all commercial enterprises, regardless of their legal form, are subject to a comprehensive set of laws, regulations, and governmental decrees [as illustrated in Exhibit 61.6]."

61.6 EFFORTS TO IMPROVE CORPORATE GOVERNANCE

Russia's corporate governance shortfalls are typical of many transitional economies in which governance is seen as a necessary evil and cost of business. But consider how far Russia has come over the Soviet Union era when MBAs and chartered and certified accountants were oddities and Western concepts of corporate organization and finance were met with contempt and/or poorly understood.

There has been some progress by many Russian companies in improving the role of corporate boards:

- Creating new corporate governance standards and policies
- Increasing decision-making roles as deal, acquisition, and merger activities grow
- Creating specialized committees for auditing, strategy, compensation, and so on
- Expanding the numbers of independent board members
- Transitioning beneficial owners from operating control to strategic planning[9]

In 2005, three regulatory agencies proposed measures to improve corporate governance—the State Duma's Property Committee, the Economic Development

Law / Regulation	Applicability	Comments
Civil Code	All commercial entities	Regulates basic governance framework
Company Law	Joint stock companies (JSCs)	Regulates founding, operation, and liquidation/reorganization of JSCs
Securities Law	JSCs that have publicly issued securities	Regulates procedures of issuance and circulation of securities; information disclosure
FCSM Regulations	JSCs that have publicly issued securities	Expands upon the company and securities law
Secondary Regulations (Tax, Bankruptcy, Etc.)	All commercial entities	Regulates specific issues for commercial entities
Listing Requirements	JSCs listed on a stock exchange	Regulates access to trading for issuers and investors

Source: IFC, March 2004.

EXHIBIT 61.6 RUSSIA: PRINCIPAL LAWS AND REGULATIONS IMPACTING CORPORATE GOVERNANCE

and Trade Ministry (EDTM)'s Expert Council on Corporate Governance, and the Federal Service for Financial Markets. The recommendations include:

- Downsizing the number of executive directors with the goal of distancing them from managerial structures
- Barring company executives from being elected to control commissions
- Improving the voting process to increase minority participation (There are 188,000 minority shareholders owning over $3 billion in stock.)
- Improving board independence and reducing conflicts of interest by amending the federal law on joint stock companies
- Reducing insider information and market manipulation by state Duma legislation that clearly defines insider information[10]

Russia's 2002 Corporate Code of Conduct is also undergoing a transformation to increase board independence, and to improve the quality and transparency of consolidated financial statements in accordance with international accounting standards.

Transparency is improving, according to Standard & Poor's, citing a domestic business improvement of 40 percent to 50 percent from 2003 to 2005. But

there are major cultural obstacles to improving transparency in a society that sees major risks in providing financial results.[11]

61.7 CONCLUSION: THE BUSINESS CASE FOR IMPROVED CORPORATE GOVERNANCE

Continuing to improve Russia's corporate governance is in almost everyone's best interest—even most of those who are currently prospering under the current state of limited governance.

Good corporate governance is important on a number of different levels:

- Provides better and cheaper access to capital
- Outperforms poorly governed peers over the long term
- Reduces risks inherent to an investment in a company
- Adds greater value for shareholders, employees, customers, and communities
- Minimizes the risk of fraud through improved accounting transparency
- Exposes internal control problems at an earlier stage to head off disasters
- Improves oversight of executive performance
- Improves the decision-making process, resulting in more timely and better-quality decisions
- Enhances the efficiency of the financial, business, and technical operations across the enterprise
- Lowers capital expenditures, contributing to potential sales and profit growth
- Facilitates the resolution of corporate conflicts at the board, management, and shareholder levels
- Lowers the chances of going to jail or being sued by ensuring compliance with applicable laws and regulations

While it is hard to argue with Russia's very real success in sustaining high economic growth rates, this is very much a transitional situation. As the Russian economy becomes more interdependent with its EU neighbors, the need for much enhanced corporate governance will grow.

Russia's sovereign democracy approach ignores the success and hard lessons learned in the West. It is analogous to the American arrogance that has ignored successful governance models (UK's Combined Code, and Australia's ASX 10) and delayed adopting principle based accounting standards (IFRS). This combined with a convoluted tax code has led to massive accounting scandals and to panicked and major regulatory overreactions in the United States.

Notes

1. Guy Chazan, "Investors Credit Putin as They Pile Up Profits: Hot Stock Market Makes Russian Leader a Hero with Money Managers," *Wall Street Journal*, January 22, 2007, A1.
2. Ibid.

3. David Satter, "Who Killed Litvinenko?," *Wall Street Journal*, November 27, 2006, A12.
4. Oleg Orlov, March 27, 2003, interview (a leader of "Memorial," Russia's leading human rights organization). November 18, 2006.
5. Ria Novosi, "What Russia Has to Offer Foreign Investors," *Post Chronicle*, November 30, 2006.
6. "The Fog of the 'New Cold War': And Guess Who's Winning So Far," *Economist.com*, December 7, 2006.
7. "Bracing for a Rough Patch," *Financial Express*, December 27, 2007.
8. U.S. Department of Commerce, International Trade Administration, "The Corporate Governance Manual," www.ita.doc.gov/goodgovernance/CorpGovManual.asp.
9. Sergei Porshakov, "Improving Corporate Governance in Russia and the EU," *Russia in Global Affairs* 2, April–June 2006.
10. Ibid.
11. "Standard & Poor's Commentary: Corporate Governance in Russia Still Constrained by Ineffective Law and Concentrated Ownership," Standard & Poor's, November 15, 2005.

CHAPTER 62

CORPORATE GOVERNANCE: SOUTH KOREA

Jill Solomon, PhD

62.1 INTRODUCTION

Corporate governance in South Korea has undergone substantial reform in recent years. The Asian financial crisis focused attention on corporate governance weaknesses in Asian companies. In the wake of the financial crisis, countries in the region have focused attention on improving and tightening their systems of corporate governance and corporate control. As outlined in Solomon (2007), South Korea has witnessed substantial economic and political change in recent years. The political environment has been liberalized and the political strategy has been to open up the South Korean economy to international investment. President Kim Dae-jung's policy of *segyehwa* (globalization) focused on making Korean businesses more internationally competitive and more attractive to foreign investors (Ungson, Steers, and Park 1997). As stressed by the Organization for Economic Cooperation Development (OECD) (2004), attracting international investment by financial institutions is one of the primary motivations for countries to reform their systems of corporate governance. Institutional investors will be more attracted to purchasing the shares of companies which have comparable corporate governance standards and practice, consistent with international standards.

This chapter provides a summary of the ways in which corporate governance in South Korea has been reformed and the problems which engendered

a programme of corporate governance reform. This chapter aims to provide a picture of how corporate governance is evolving in South Korea. The focus is on a number of issues relating to corporate governance in South Korea, specifically:

- The traditional framework of corporate governance in South Korea
- The recent agenda for corporate governance reform in South Korea
- Empirical evidence relating to corporate governance reform in South Korea

In the concluding section, there is a discussion of the need for continuing reform, despite evident and effective progress to date. This is especially important if there is any hope in the future of unifying the Korean peninsula, as corporate governance in South Korea is likely to be used as a template for the eventual corporate governance system in a unified Korea.

62.2 TRADITIONAL FRAMEWORK OF CORPORATE GOVERNANCE IN SOUTH KOREA

There are as many different systems of corporate governance as there are countries in the world (Solomon 2007). The principal factors which determine a country's corporate governance framework are corporate ownership structure, legal framework, and other characteristics such as culture and politics. In South Korea, the corporate governance system has traditionally been determined by ownership structure, legal environment, and state intervention.

The corporate community in South Korea has traditionally been dominated by large conglomerate groups known as *chaebol*. These conglomerate business groups evolved from small, family-run businesses, which expanded exponentially, but which remained under the control of the founding families. This traditional corporate ownership structure in South Korea has meant that the corporate governance framework fitted neatly into the insider-dominated model of corporate governance (Solomon 2007). This model is characterized by owners (often families, as in the case of South Korean *chaebol*) who also control the corporation. In the case of South Korea, the *chaebol* have also been heavily influenced by the state, with government frequently setting the corporate agenda on choice of production and corporate strategy. Although such obvious alignment of ownership and control implies an absence of the notorious agency problem, insider systems of corporate governance such as that found in South Korea are typified by other types of problems. Abuses of power and lack of transparency are often associated with insider-oriented corporate governance systems.

Due to cultural influences in South Korean business, the *chaebol* have grown as hierarchical business structures. Confucian ethics has traditionally promoted a hierarchical business (as family) environment and this has led to strong, dominant leadership within the *chaebol* (see Song 1997; Solomon et al. 2002a). Abuses of power, lack of transparency, and other corporate governance weaknesses were

blamed in part for the way in which South Korea succumbed to the Asian crisis in 1997, as stated in the Digital *Korea Herald* (2000);

> . . . anachronistic activities by chaebol were part of what caused Korea's economic crisis. . . .

Indeed, Balino and Ubide (1999) emphasized that the lack of transparency and accountability demonstrated by the *chaebol* has been blamed for the way in which South Korea succumbed to the financial crisis in Asia (see also Kim 2000). In the following section we discuss some of the problems inherent in the traditional corporate governance system in South Korea as well as the steps taken to reform corporate governance in these areas.

62.3 CORPORATE GOVERNANCE REFORM IN SOUTH KOREA: REFORMING OWNERSHIP STRUCTURE

Due to the dominance of founding family ownership in South Korean business, more than 80% of company shares were held by less than 2 percent of shareholders in 1996 (OECD 1999). This ownership structure has been accompanied by weak investor protection for minority shareholders, a problem inherent in insider-dominated economies. The German/Scandinavian-derived legal framework adopted in South Korea exacerbates this problem, as it notoriously does not afford high protection to shareholders (see La Porta et al. 1997; Solomon 2007). It important to stress that institutional investor ownership in South Korea is around 35 percent rather than the high proportions in countries like the United Kingdom (over 70 percent).

Ensuring equal treatment of all shareholders has been one of the primary aims of the OECD (2004) principles for good corporate governance. As a result of pressures to harmonize corporate governance standards globally, the South Korean government has therefore focused on broadening corporate ownership by nurturing an equity culture, at the same time strengthening investor protection through changes in the Commercial Code. This is typical of the approach taken to reform corporate governance in countries with codified legal structures. Whereas in the UK and other common law countries, voluntary codes of practice and policy documents suffice to push through changes in corporate governance, countries with codified legal structures have had to formally change the legal framework in order to change corporate governance practices (Solomon 2007). In recent years, the *chaebol* have significantly reduced their debt-equity ratios, mainly through increasing equity ownership (Solomon et al. 2002a).

There has been a significant rise in shareholder democracy in South Korea which has also helped to push through changes in corporate governance, especially in relation to the more equitable treatment of minority shareholders. As stated in Kim (2000, 312),

> Upon realizing that they have rights, shareholders are becoming more active participants in corporate affairs.

The People's Solidarity for Participatory Democracy (PSPD) is an important civic group which has targeted companies and lobbied for greater corporate transparency and accountability. For example, the PSPD urged Hyundai to compensate its customers for losses arising from the illegal transfer of bad securities to their trust funds (see Solomon et al. 2002a). Such shareholder intervention was unheard-of in South Korea until recent years.

Another sign that minority shareholders rights are being improved in South Korea is the legal change removing limitations to institutional investors' voting rights in 1998 (Solomon et al. 2002a). Percentage limits on voting have also been lowered, allowing larger number of shareholders to exercise their right to vote (Kim 2000). For institutional investors, the situation has improved significantly as they are now no longer restricted to shadow voting for customer accounts (see Hong and Lee 1998; Lee 1998). However, it has been acknowledged that shareholders in South Korea did not want involvement in corporate governance until recent times, although this is probably attributable to ignorance of their potential rights and responsibilities (Kim 2000).

Another way in which Korean shareholders' rights have been improved is through reform of the annual general meeting (AGM). As explained in Solomon et al. (2002a), one characteristic of insider-dominated stock markets is the tendency for companies to organize their AGMs so that they all take place at the same time on the same day. This has obvious repercussions on shareholder democracy, as shareholders cannot be in more than one place at a time. In 2000, 224 out of 406 Korean companies held their AGMs on the same day, which indicates the scale of the problem. This has changed significantly in recent years, with the PSPD pressuring companies to hold AGMs that allow greater shareholder attendance and involve extensive shareholder discussion. As stated in Kim (2000, 311–312),

> Shareholder rights have been strengthened to levels previously unimaginable by Korean standards.

62.4 TRANSPARENCY AND BOARD STRUCTURE

There also have been significant moves toward greater transparency by the South Korean *chaebol*. Lack of transparency in succession arrangements, for example, had led to grave concerns about the *chaebol*'s accountability and transparency (see, for example, the case of Hyundai in Solomon et al. 2002a). The hierarchical structure of South Korean business has led to criticisms of excessive top-heavy and family-dominated board structures. The *chaebol* have made great strides in dismantling top-heavy decision-making bodies, replacing them with structures which allow greater delegation of power and more democratic decision making (Solomon et al. 2002a).

Lack of independent voice in the boardroom provides opportunities for unethical boardroom practices and lack of transparency. In recent years, the

agenda for corporate governance reform in South Korea has involved the introduction of independent board members into the boardroom. Since 1999 all listed companies have been required to have at least a quarter of their boards consisting of independent directors (Solomon et al. 2002a). Again, the PSPD has been instrumental in calling for South Korean *chaebol* to integrate independent directors into their board structures.

An essential element of corporate transparency is of course the accounting and financial reporting function. South Korea has focused on improving corporate transparency through clearer disclosure of financial statements. For example, in the past few years, Korean *chaebol* have been forced to produce mandatory combined financial statements and quarterly reporting, based on International Accounting Standards (IAS) (see Solomon et al. 2002a).

Solomon et al. (2002a) summarize the South Korean corporate governance framework and identify the forces driving South Korea toward corporate governance reform in diagrammatic form. The principal drivers of corporate governance reform arise from the shareholders, from the government, and from external bodies. As we saw earlier, shareholder activists such as the PSPD have recognized serious weaknesses in the corporate governance of the *chaebol* and have lobbied for reform. The *chaebol* corporate governance structure has been recognized as outdated and not in line with international standards and principles of good corporate governance practice. Especially in the area of shareholder rights, the shareholder community in South Korea has been active in bringing about change. The government, recognizing a need for South Korea to adopt internationally acceptable corporate governance standards in order attract foreign capital, has pushed the *chaebol* toward greater transparency and better corporate governance. As well as pressures from foreign financial institutions, the OECD itself has helped to drive corporate governance reform in South Korea. The country's accession to the OECD has forced it to adopt the OECD principles for good corporate governance.

62.5 EMPIRICAL EVIDENCE RELATING TO CORPORATE GOVERNANCE REFORM IN SOUTH KOREA

Institutional investors have been acknowledged in the literature as an essential mechanism in promoting better corporate governance (Solomon 2007). Some research has examined the extent to which corporate governance reform in the light of the Asian crisis has improved the mechanism of institutional investor activism in South Korea. There is strong evidence that the influence of foreign equity investment into South Korea has been significant since the Asian crisis and that this has aided the economy's journey toward a more Anglo-Saxon style of corporate governance, which is modeled on the OECD principles (2004) (see Yanagimachi 2004). Solomon, Solomon, and Park (2002b) outline the findings of a questionnaire survey that canvassed the views of institutional investors in South Korea concerning corporate governance and corporate governance reform. The

study found positive indications that Korean institutional investors were becoming increasingly interested in corporate governance in South Korea and that they perceived they had a growing role in terms of responsibility and exercise of their rights. Indeed, Solomon et al. (2002b, 222) conclude that:

> . . . the institutional investors' role in corporate governance reform is becoming increasingly important—they are essential tools in the reform machinery.

The institutional investors who participated in the research indicated on the whole that they wanted to be actively involved in their investee companies' business activities and decision making. They also were keen to be more activist and wanted to exercise their voting rights. However, the research did reveal that despite significant improvements in shareholder activism, institutional investors were still not implementing their voting rights as widely as anticipated, given the reforms which have occurred. There is clearly a long way to go in terms of education and raising awareness before institutional investors become as active in exercising their rights in South Korea as they are other more developed corporate governance systems.

In the wake of the Asian crisis and attempts to reform corporate governance in South Korea, some research has examined the impact on board effectiveness. Chang and Shin (2006) found empirical evidence to support the view that the effectiveness of the governance of *chaebol* has in fact been improved. They argue from their empirical research that even those conglomerates which were among the worst performers, in terms of corporate governance, have improved their governance dramatically since the Asian crisis. There is also evidence that since the crisis and the emergence of an agenda for corporate governance reform, many *chaebol* have disappeared (Hyundai and Daewoo being among the victims of reform and globalization) (see Yanagimachi 2004). This is partly because they have not been able to compete globally. Change is never easy, and the efforts of South Korea to become a globally competitive economy, with global corporate players, attracting global capital, were bound to engender some casualties in the corporate sector.

62.6 CONCLUDING COMMENTS

It is quite clear from the short summary of evidence in this chapter that corporate governance reform has come a long way since the Asian crisis in bringing South Korea up to speed and in line with international standards of corporate governance best practice. The accession of South Korea into the OECD in the late 1990s has helped to accelerate corporate governance reform, as has the significant impact of the Asian financial crisis. Corporate governance in South Korea has moved some way toward a more Anglo-Amercian style of corporate governance, with its own code of practice modeled on the OECD principles (2004). However, whether Anglo-Saxon corporate governance is the appropriate model for a country with such different cultural characteristics, history, and politics is debatable. As with

all emerging stock markets, a blatant adoption of the dominant Anglo-American model is not necessarily the most appropriate or politically correct approach. However, for South Korea to become a truly successful global competitor, it is likely that adopting the Anglo-American style governance is the only option. As argued by Yanagimachi (2004),

> Creating an Anglo-American corporate governance system will be difficult without an understanding of the Korean business landscape that such governance must be imposed on: factors such as the traditional aspects of chaebols, the stance of Korean government that is characterized by its forcible intervention into the management of chaebols, and the issue of radical labor unions. It is, however, essential that the Anglo-American corporate governance system be harmonized with the Korean business landscape if an internationally competitive corporate society is to flourish in Korea.

Further, in a broader context, if there is going to be a definitive move in the future toward a unified Korea, then continuing improvements in the corporate governance framework in South Korea are essential, as the South Korean economic system is likely to be the role model for the unified country and for the privatization of North Korea (see Milhaupt 1999).

References

Balino, T. J. T., and A. Ubide. 1999. The Korean financial crisis of 1997—A strategy of financial sector reform. IMF Working Paper WP/99/29.

Chang, J. J., and H-H. Shin. 2006. Governance system effectiveness following the crisis: The case of Korean business group headquarters. *Corporate Governance: An International Review* 14, no. 2 (March): 85–97.

Digital Korea Herald. 2000. Top financial regulator rejects chaebol demands for regulation. April 27.

Hong, S., and J. Lee. 1998. Institutional investors to be granted voting rights. *Joongang Ilbo*, February 7.

Kim, J. 2000. Recent amendments to the Korean commercial code and their effects on international competition. *University of Pennsylvania Journal of International Economic Law* 21: 273–330.

La Porta, R., F. Lopez-de-Silanes, A. Shleifer, and R. W. Vishny. 1997. Legal determinants of external finance. *Journal of Finance* 52 (3): 1131–1150.

Lee, J. 1998. The role of institutional investors in listed companies. *Commercial Law Review* 17 (151): 167–177.

Milhaupt, C. J. 1999. Privatization and corporate governance: Strategy for a unified Korea. Working Paper 160, Columbia Law School.

OECD. 1999. *Economic survey, Korea*. Paris: OECD.

OECD. 2004. *OECD principles of corporate governance*. Paris: OECD.

Solomon, J. F. 2007. *Corporate governance and accountability*. 2nd ed. Hoboken, NJ: John Wiley & Sons.

Solomon, J. F., A. Solomon, and C. Park. 2002a. A conceptual framework for corporate governance reform in South Korea. *Corporate Governance: An International Review* 10 (1) (January): 29–46.

Solomon, J. F., A. Solomon, and C. Park. 2002b. The role of institutional investors in corporate governance reform in South Korea: Some empirical evidence. *Corporate Governance: An International Review* 10 (3) (July): 211–224.

Song, B-N. 1997. *The rise of the Korean economy*. New York: Oxford University Press.

Ungson, G. R., R. M. Steers, and S-H. Park. 1997. *Korean enterprise: The quest for globalization*. Boston: Harvard Business School Press.

Yanagimachi, I. 2004. Chaebol reform and corporate governance in Korea. Policy and Governance Working Paper 18, Graduate School of Media and Governance, Keio University, Japan, February.

CHAPTER 63

CORPORATE GOVERNANCE: SPAIN

Anthony Tarantino, PhD

63.1 INTRODUCTION

Spain has enjoyed one of the hottest stock markets in the past year as wealthy Spanish investors have driven up the value of blue-chip stocks. Spain's 2006 IBEX-35 index growth rate of 32 percent was twice that of France's CAC-40 and two and one half times that of London's FTSE-100. This heated growth may be dampened in 2007 by pending changes to takeover law in which stockholders are required to bid for the remainder of a company once their portion exceeds 30 percent—down from 50 percent under the current rules.[1]

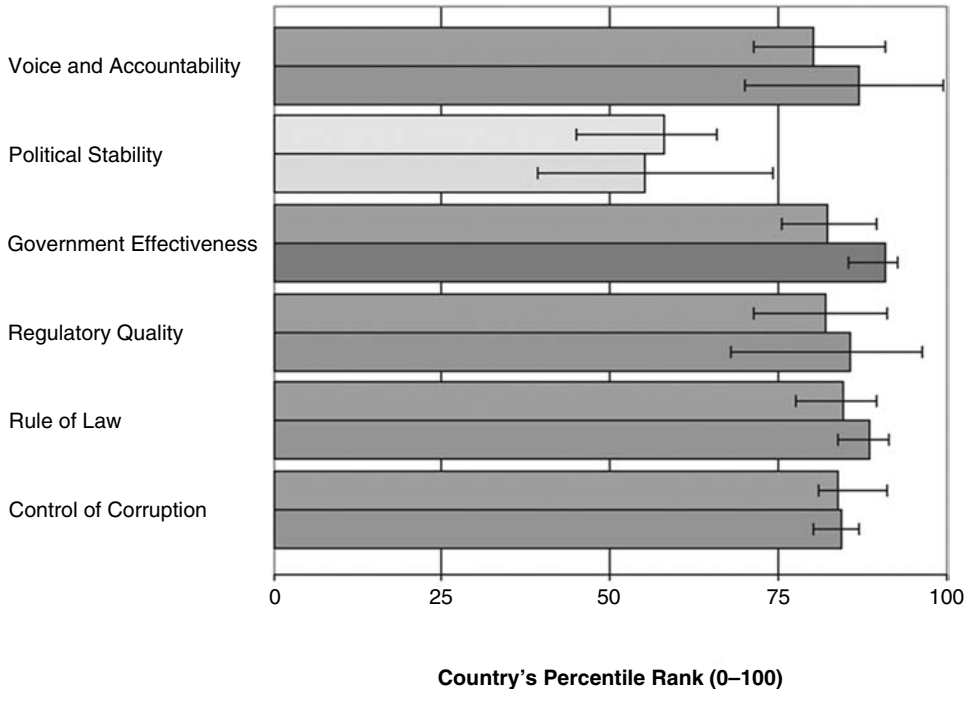
Spain has emerged as a major player in new markets with companies such as Telefónica SA, Ferrovial SA, and Abertis SA leading the way with aggressive acquisition and merger strategies. With its high growth rates, job creation, and financial and political stability, Spain joins Britain, France, and Germany as a major EU economic power.[2]

Spain has also progressed ahead of many other EU members by deregulating telecommunications, banking, and energy industries while gaining valuable expertise by its *reconquista* expansion into Latin America over the past decade. Spanish tax laws give breaks to foreign-acquired goodwill, which reduces purchase costs, encouraging cross-border deals. This along with its growing financial expertise has increased cross-border acquisitions.[3]

63.2 CURRENT STATE OF CORPORATE GOVERNANCE

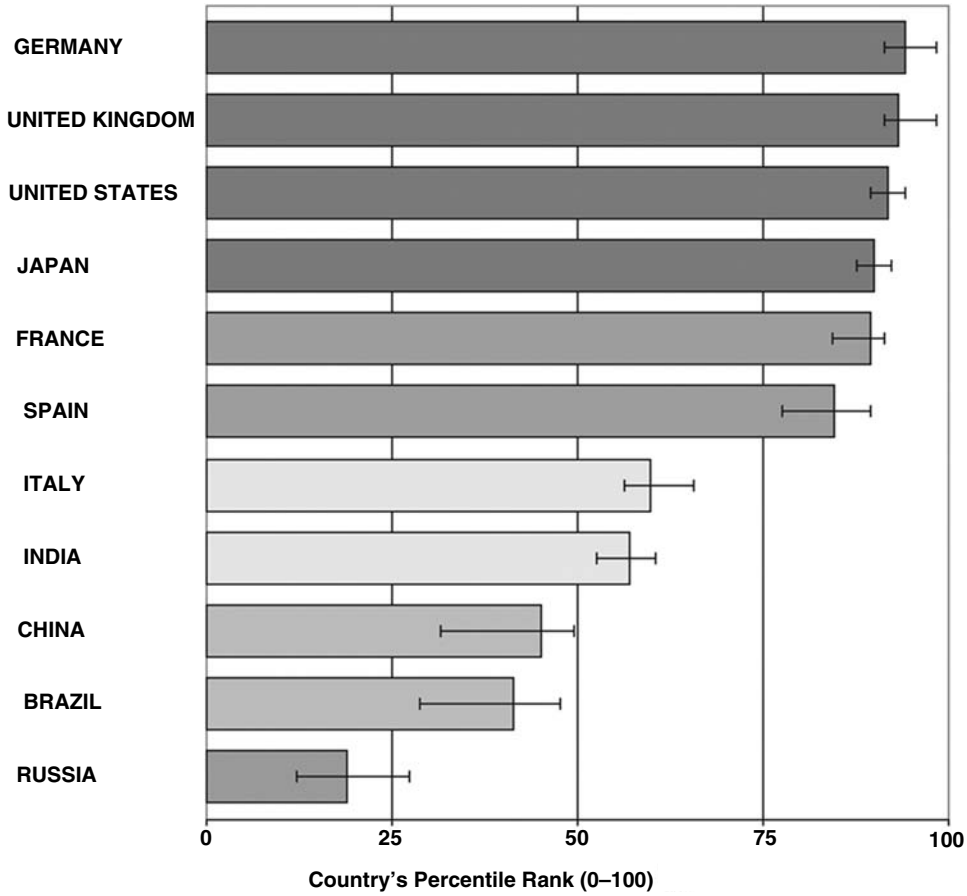
The World Bank publishes country-to-country and year-to-year evaluations covering six areas of governance. By these measures, Spain's performance is quite impressive. Spain ranks fourth in regulatory quality, fifth in control of corruption, and sixth in the rule of law when compared to the world's leading economies. It has declined in only one category over the past nine years—political stability/no violence. (See Exhibits 63.1 to 63.4.)

Heidrick & Struggles' 2005 Corporate Governance Study echoes the World Bank findings. They note strong evidence of broad-based corporate governance improvements, with Spain moving from ninth to sixth in its Europe rankings. The study does caution that there are still challenges in standardizing governance legislation—the 1988 Livencia Report needs to reconciled with the 2003 Aldama Report.[4]



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 63.1 WORLD BANK GOVERNANCE RANKINGS: SIX AREAS OF GOVERNANCE FOR SPAIN 2006 AND 1996 (TOP-TO-BOTTOM ORDER)



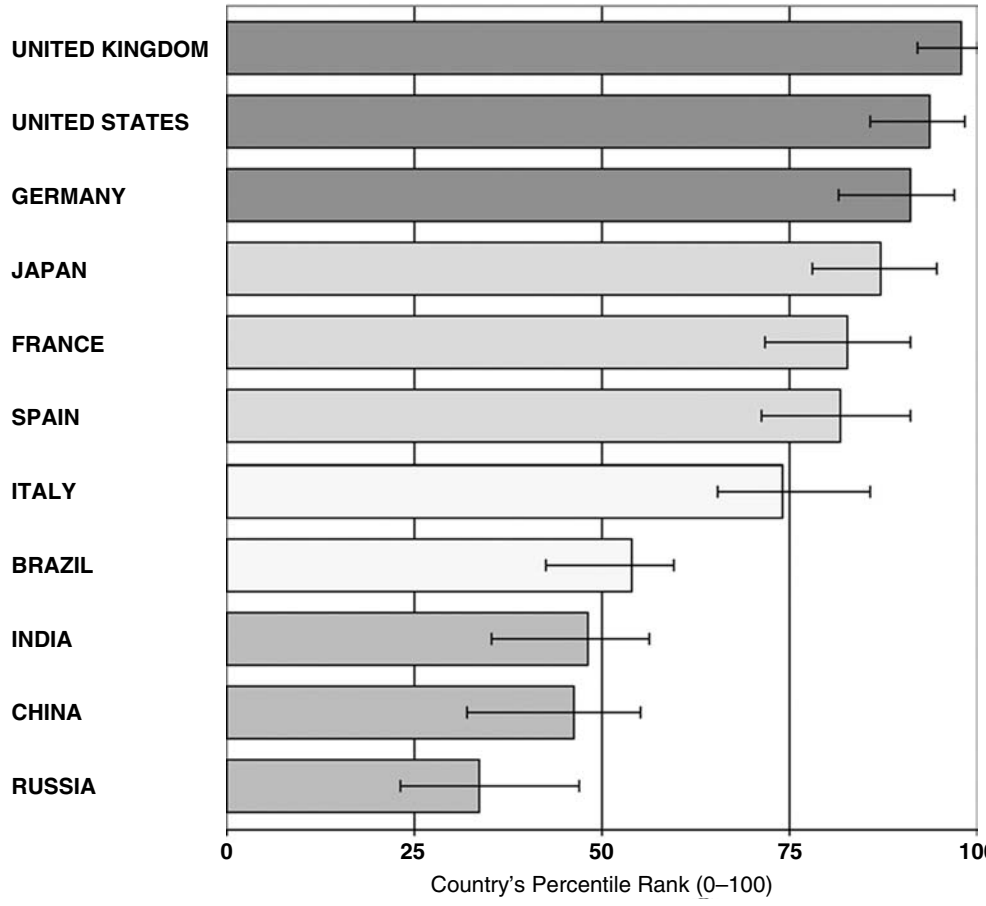
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 63.2 WORLD BANK GOVERNANCE RANKINGS: RULE OF LAW FOR SPAIN AND MAJOR GDP NATIONS

Spain's governance model parallels somewhat those of Italy and Spain:

- Concentrated firm ownership
- Strong intervention by the state
- Weak company-level labor participation
- A growing role for foreign multinationals

But Spain is forming its own unique hybrid approach adopting portions of UK standards. State ownership is declining due to privatization and the influx of foreign capital. This decline has witnessed a corresponding increase in



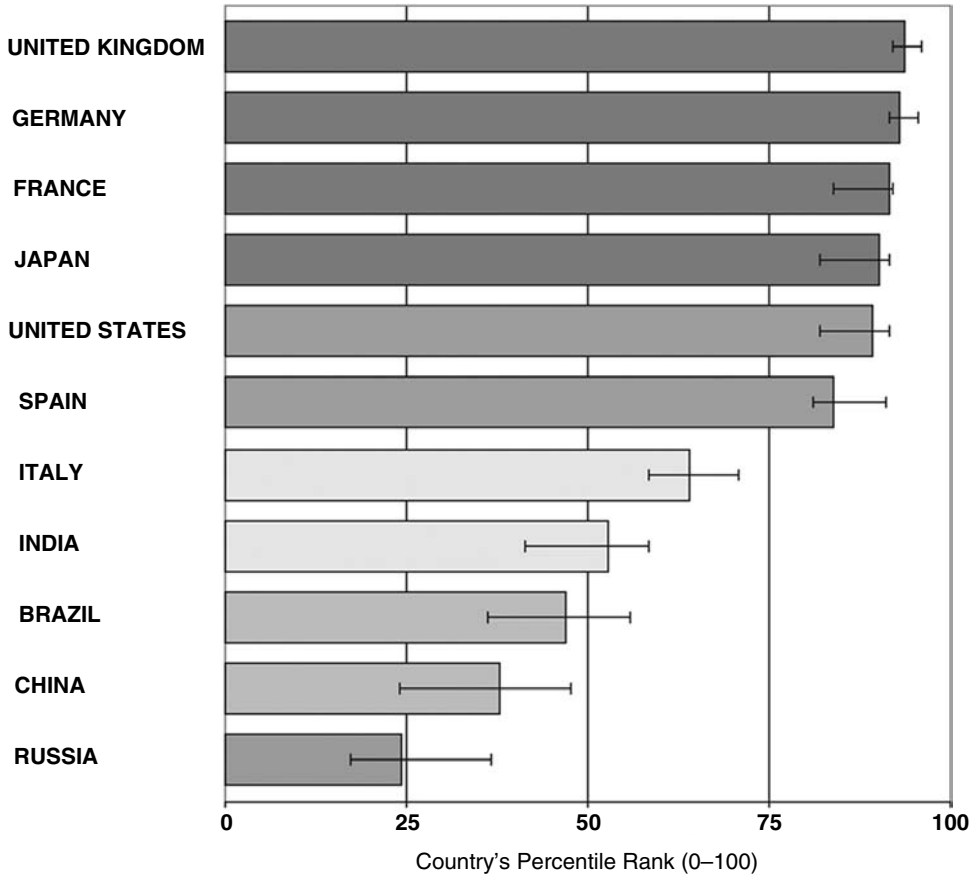
Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 63.3 WORLD BANK GOVERNANCE RANKINGS: REGULATORY QUALITY FOR SPAIN AND MAJOR GDP NATIONS

nonfinancial firm ownership—30 percent of total equity is now held by private households. This is roughly double UK and German rates.[5]

The Heidrick & Struggles' 2005 study summarizes Spain's governance in its present state as follows for the 35 IBEX companies:

- A continuing reluctance to provide board salary and age data
- A minimum of two committees per company—major improvement over the past five years
- Audit committees in all member companies, which on average meet over seven times per year—higher than the EU average
- Compensation committees in virtually all member companies



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (July 2007).

EXHIBIT 63.4 WORLD BANK GOVERNANCE RANKINGS: CONTROL OF CORRUPTION FOR SPAIN AND MAJOR GDP COUNTRIES

- Less than half of member companies possess an independent committee chairman
- Very poor representation of women board members—under 3 percent[6]

63.3 THE ALDAMA REPORT, TRANSPARENCY ACT, AND CNMV REGULATIONS

In 2002 the Spanish government commissioned a report on improving corporate governance. In January 2003 the Aldama Commission issued its recommendations to improve governance, transparency, and the security of financial markets. The recommendations include proposed legislature reforms as well as actionable recommendations for companies. The Aldama Report was fairly well received

and passed as the Transparency Act in July 2003. The regulations to enact the legislation were developed by ministerial order and by the Spanish Securities and Exchange Commission (CNMV).

CNMV regulations to enforce the Transparency Act include:

- Companies have to pass an annual corporate governance report, whose content is very much in line with the annual corporate governance report envisaged in the High Level Group of Company Law Experts Report, know as the Winter Report.
- Web-based publishing of all relevant financial reports.
- Support for minority shareholder rights to information.[7]

63.4 BOARD OF DIRECTORS AND BOARD COMMITTEES

Historically and legally Spain follows a one-tier board structure. Typically boards delegate powers to directors or to an executive committee. The executive committee is a popular means for boards to delegate authority. The Financial Measures Act of 2002 requires the creation of an audit committee reporting to the board of directors for all publicly listed companies. Under the new legislation, audit committees are required to:

- Contain a majority of non-executive directors
- Be run by a president who is a nonexecutive director
- Report and answer to shareholders as to their expertise and experience
- Propose the appointment of external auditors
- Supervise internal audit activities
- Be knowledgeable in the preparation of financial information
- Be knowledgeable in internal control systems used by the company

The Stock Markets Law of 2003 recommends the creation of remuneration and compensation committees. Following the UK model, companies are required to either comply or explain why these committees are not needed. These committees must be made up of a majority of independent directors. While companies are given flexibility in complying with these regulations, all must pass board regulations that cover the internal board workings.[8]

The Companies Act of 2003 (LSA) imposes the same fiduciary and due diligence requirements on executive and nonexecutive directors, but does not clearly define the differences between the two roles. It is clear that a nonexecutive director can be neither an independent director nor a proprietary director—a director who is appointed by a major company shareholder.

Director compensation is addressed at least partially in the LSA. Regulations describe variable compensation tied to a company's profits and stock option plans. Given the exploding U.S. scandal over options and ease of manipulating option dates, Spanish companies may be well advised to consider other

pay-for-performance alternatives. The corporate governance report advocates the global disclosure of director compensation. Governance commissions and many companies are publishing the individual remuneration of each director.

Unlike the United States, which places the burden for financial reporting on CEOs and CFOs (Section 302 of the Sarbanes-Oxley Act), Spanish law places this burden on directors. The Aldama Report makes recommendations that mirror the U.S. Sarbanes-Oxley Act in that financial reports are to be certified by CEOs and CFOs. There is a very valid argument for placing this burden at the board level as well as the CEO and CFO level. Such an arrangement creates a strong system of checks and balances and minimizes the chances for fraud or error. Most directors do not want to risk damaging their reputations and will be highly motivated to assure the accuracy of financial reports.

63.5 AUDIT REGULATIONS

Audit firms have come under greater control with the Financial Measures Act (LMF) of 2002. The act is generally faithful to the European Commission's general guidelines requiring the independence of auditors. Audit firms continue to fall under the authority of the Instituto de Contabilidad y Auditoría de Cuentas (ICAC). The LMF forbids auditors from:

- Acting in a managing role in the audited company, or companies related to the audited company.
- Having a financial interest in the audited company.
- Having family relationship with managers in the audited company.
- Preparing the financial accounts of the audit company.
- Designing the audited company's information technology systems for the processing of financial information.
- Performing appraisal or valuation services for the audited company.
- Assisting the audited company's internal audits.
- Acting as an advocate for the audited company.
- Assisting in selecting executives in the audited company.
- Becoming directors in the audited company for three years following the audits.
- Permitting the same partner to perform both consulting and audit services for the same company. The law permits the audit firm to do both within some limits.
- Permitting the same partner and partner team to audit the same company for more than seven years. There is no rotation requirement for the audit firm itself.

These final two prohibitions are not adequate to prevent abuse. Arthur Andersen and Enron are the best proof of the need to rotate audit firms and to avoid conflicts of interest in selling both auditing and consulting services.

Rotating firms permits a fresh set of eyes to review financial results and will keep audit firms on their toes knowing a competitor is going to review their work. Audit firms selling consulting services to a client they audit is a bad idea. The conflicts of interest are very obvious and the greed potential too great to prevent abuse by even the most ethical of audit partners.

63.6 CORPORATE GOVERNANCE DISCLOSURE

The annual corporate governance report and the company's web page are the primary vehicles for disclosing governance and operational information. Both the Winter Report and the Aldama Report laid the foundation for the current process, which was enacted into law in 2003 as s116 LMV. It requires an annual filing to the Securities Commission containing:

- The structure of ownership of the company such as substantial shareholdings
- Relationships between significant shareholders, and their presence in the board of directors
- Shares held by members of the board of directors
- The existence and contents of shareholder agreements that are known by the company
- Data related to company's own shares and dealings in the company's own shares
- The structure and membership of the board
- Rules governing the board and its committees
- Compensation of the board members
- Board member relationships with significant shareholders
- Board members who are members on other boards
- Procedures for board member selection, reelection, and removal
- Related-party transactions, including operations with shareholders or directors of companies belonging to the same corporate group
- Risk control systems in place and planned
- Procedures and processes for running shareholder meetings
- The level of governance compliance recommendations and explanations when recommendations are not followed

The company's web page is an important tool in public disclosure and transparency. It should include the annual corporate governance reports, press releases, minutes of shareholder meetings, articles, and White Papers.

63.7 THE BANKING SECTOR

The two largest banks in Spain are emerging as global players with profit margins that exceed some of the largest global players. Banco Bilbao Vizcaya Argentaria SA (BBVA) is making major U.S. acquisitions to challenge Bank of America and JPMorgan Chase in the South and West. In 2006, Banco Santander

Central Hispano SA acquired 25 percent of a New England bank with over 700 branches. These and other acquisitions have made BBVA and Santander the 15th and 9th largest banks respectively as measured by market share. They are also among the world's most profitable banks. Both enjoy returns on equity over 20 percent—rates above HSBC, Bank of America, and Citi.[9]

Strong domestic competition compelled both banks to invest heavily in efficiency improvements, technology, and operational risk management—all essential in meeting the Basel II capital accords. The capital adequacy of Spanish banks is regulated by both the EU directives applicable to the Spanish banking system and by the banking systems of other EU member states. Many of the larger EU member states have signed on to the Basel accord. Spain decided to join the Basel accord in early 2001. Basel is not a regulation and must be coded by each nation's banking authority. Basel's capital requirements are very much in line with the EU capital directives, Spanish regulations, and the Bank of Spain.

Both banks are making progress in operational risk measurement, as part of their plan to apply the advanced measurement approach (AMA) required by Basel II for the calculation of capital charges for operational risk.

63.8 CONCLUSION

Spain has made significant process in improving corporate governance and can be viewed as a role model in demonstrating that high growth and competitiveness are not at odds with good governance. The top-down approach to governance places accountability where it belongs—at the board level and the executive level. With a few exceptions, the increased oversight of companies and audit firms and the increased transparency requirements are working to improve confidence among shareholders, regulators, rating agencies, employees, suppliers, customers, and communities. Spain's Securities and Exchange Commission, the CNMV, has the expertise and willpower to facilitate the journey to improved governance to overcome some of the remaining obstacles, such as the need to consolidate the older Livencia Report (1988) with the newer Aldama Report (2003).

Some other recommendations include:

- Mandatory rotation of audit firms every few years.
- Stricter prohibitions against audit firms selling consulting and tax services.
- More clearly defining the roles of executive and nonexecutive directors.
- Increasing the participation of women on corporate boards.

Notes

1. David Roman and Christopher Bjork, "Spain's Bull Run Could Slow," *Wall Street Journal*, December 28, 2006, C10.
2. Keith Johnson, "Spain Emerges as M&A Powerhouse," *Wall Street Journal*, September 26, 2006, A6.
3. Ibid.

4. Heidrick & Struggles, "Corporate Governance in Europe: What's the Outlook? 2005 Study," 30–31.
5. Ibid.
6. Ibid.
7. José M Garrido García, "Corporate Governance in Spain," report prepared for the European Corporate Governance Conference, The Hague, The Netherlands, October 18, 2005.
8. Ibid.
9. Keith Johnson, "Spanish Banks Become Major Global Players: BBVA-Compass Deal Is Just the Latest; Target: U.S. Market," *Wall Street Journal*, February 17, 2007, B1.

CHAPTER 64

CORPORATE GOVERNANCE: UNITED KINGDOM

Dennis Cox

64.1 CURRENT STATE REGULATORY COMPLIANCE OVERVIEW

(a) POLITICAL AND CULTURAL ENVIRONMENT. Within the United Kingdom, corporate governance has been enshrined in the psyche of business for decades. In common with other countries, changes to codes have generally been as a result of well-publicized cases where the government of the time has felt compelled to act.

Cadbury, Hampel, Turnbull, and Higgs all produced reports, and the Combined Code has then tried to implement these standards consistently throughout the listed sector. In this chapter it is the Combined Code on which we primarily focus and consider its impact on the UK financial community. The political imperative is quite clear. Governments of all persuasions have seen corporate governance as being a political imperative since there is no advantage to the ruling party as being soft on corporate activity.

The culture of business in the UK has always been globalist; effectively an island state has to be globalist. UK firms recognize that the world is full of markets in which they can do business. At the same time there is a public sentiment that has increasingly been seen as potentially being antiglobalist. The media may complain about a financial institution paying relatively little UK taxation on

its global income, while failing to recognize that the majority of their income is derived from abroad. There is an equal amount of envy regarding the amounts earned by directors of major companies, yet these amounts can still appear small when compared to a footballer or pop star. Basically the media has created an uneven playing field where it is easy to criticize failings of corporate governance, which fortunately have been fairly rare in the UK.

At the heart of the issue is what corporate governance in a UK context really means. Under UK company law, the board of a company has ultimate responsibility for the stewardship of that company and also to balance the various conflicting demands of the various stakeholders. These include:

- Shareholders
- Staff
- Customers
- Suppliers
- Tax authorities
- The wider public interest
- Regulatory bodies

Each of these is looking for something different from the board. Corporate governance is about taking these conflicting requirements fully into account when designing a control and procedural structure that is suitable for the business. As such, UK corporate governance codes have tended to be relatively benign documents that provide a set of guidance without formally requiring very much.

These codes are generally designed to focus on the narrowness of procedure rather than true governance. Nothing in a corporate governance code actually requires a business to make the right analysis of its trading position, its advantages and disadvantages; rather they tend to focus on the level of oversight that is considered as being required by so-called independent individuals.

Whether this actually adds very much value we will consider in the section on people later.

(b) LEGAL ENVIRONMENT. UK listed companies are required to include a statement on corporate governance in their annual reports. These reports are based on the standards within the Combined Code.

The current Combined Code on Corporate Governance was issued in June 2006 by the Financial Reporting Council and replaced the Combined Code issued in 2003 and contains main and supporting provisions. The Listing Rules require listed companies to make a disclosure statement in two parts in relation to the Code. In the first part of the statement, the company has to report on how it applies the principles of the Code. The actual form and content are not prescribed by the rules. In the second part the company has either to confirm that it complies with the Code's provisions or, where it does not, to provide an explanation. This idea

of comply or explain goes back at least ten years within corporate governance rules, and generally is enshrined within the way business if conducted in the UK.

We will look at a few examples of UK corporate governance statements later.

The main principles of the Code are:

A. Directors

A.1 The Board

Every company should be headed by an effective board, which is collectively responsible for the success of the company.

A.2 Chairman and Chief Executive

There should be a clear division of responsibilities at the head of the company between the running of the board and the executive responsibility for the running of the company's business. No one individual should have unfettered powers of decision.

A.3 Board Balance and Independence

The board should include a balance of executive and nonexecutive directors (and in particular independent nonexecutive directors) such that no individual or small group of individuals can dominate the board's decision making.

A.4 Appointments to the Board

There should be a formal, rigorous, and transparent procedure for the appointment of new directors to the board.

A.5 Information and Professional Development

The board should be supplied in a timely manner with information in a form and of a quality appropriate to enable it to discharge its duties. All directors should receive induction on joining the board and should regularly update and refresh their skills and knowledge.

A.6 Performance Evaluation

The board should undertake a formal and rigorous annual evaluation of its own performance and that of its committees and individual directors.

A.7 Reelection

All directors should be submitted for reelection at regular intervals, subject to continued satisfactory performance. The board should ensure planned and progressive refreshing of the board.

B. Remuneration

B.1 The Level and Makeup of Remuneration

Levels of remuneration should be sufficient to attract, retain, and motivate directors of the quality required to run the company successfully, but a company should avoid paying more than is necessary for this purpose. A significant proportion of executive directors' remuneration

should be structured so as to link rewards to corporate and individual performance.

B.2 Procedure

There should be a formal and transparent procedure for developing policy on executive remuneration and for fixing the remuneration packages of individual directors. No director should be involved in deciding his or her own remuneration.

C. Accountability and Audit

C.1 Financial Reporting

The board should present a balanced and understandable assessment of the company's position and prospects.

C.2 Internal Control

The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.

C.3 Audit Committee and Auditors

The board should establish formal and transparent arrangements for considering how they should apply the financial reporting and internal control principles and for maintaining an appropriate relationship with the company's auditors.

D. Relations with Shareholders

D.1 Dialogue with Institutional Shareholders

There should be a dialogue with shareholders based on the mutual understanding of objectives. The board as a whole has responsibility for ensuring that a satisfactory dialogue with shareholders takes place.

D.2 Constructive Use of the Annual General Meeting (AGM)

The board should use the AGM to communicate with investors and to encourage their participation.

E. Institutional Shareholders

E.1 Dialogue with Companies

Institutional shareholders should enter into a dialogue with companies based on the mutual understanding of objectives.

E.2 Evaluation of Governance Disclosures

When evaluating companies' governance arrangements, particularly those relating to board structure and composition, institutional shareholders should give due weight to all relevant factors drawn to their attention.

E.3 Shareholder Voting

Institutional shareholders have a responsibility to make considered use of their votes.

Clearly these are very general principles, which any good company would normally expect to comply with. Of course there are always exceptions, but the Code has encouraged improved communication with stakeholders of the way in which corporate governance actually takes place with a firm.

There are supporting principles for each of the main provisions, which provide greater clarification of the issue under consideration. When a firm fails to comply with the Code, it is generally a supporting principle rather than the main principle that is not complied with. These areas of noncompliance are generally reported in the financial press and there can be adverse press comment, but this does not always correlate to a reduction in the market value of the company itself.

A few typical reports are:

1. *Marks & Spencer 2006 (Summary Report)* The Board is committed to high standards of corporate governance. For the year ended April 1, 2006 the Company complied with all the provisions of the Code except:

   Audit Committee Membership C.3.1 The Board should satisfy itself that at least one member of the Audit Committee has recent and relevant financial experience.

   The Board is confident that the collective experience of the Committee enables them as a group to act as an effective Audit Committee. With the appointment of Jeremy Darroch on 1 February 2006 as a nonexecutive director and Committee member, the skills and experience of the Committee as a whole have been refreshed.

   Annual General Meeting Attendance D.2.3 The Chairman should arrange for the chairmen of the Audit, Remuneration, and Nomination Committees to be available to answer questions at the AGM and for all directors to attend. Two of our nonexecutive directors, Steven Holliday and Anthony Habgood, were unable to attend the meeting in July 2005 due to previous personal commitments and business priorities, respectively.

   A statement explaining our governance policies and practices is given in the Annual Report and financial statements. A detailed account of how we comply with the Code provisions can be found on our web site at www.marksandspencer.com/investorrelations.

   This is clearly a qualified report, qualified for matters that are effectively inconsequential. Do you really think that anyone reading the report was actually concerned at the two directors' nonattendance or that the firm may not have sufficient financial experience? The Combined Code becoming more prescriptive does lead to this type of approach.

2. *Amstrad 2005*

   Corporate Governance The Board is accountable to the Company's shareholders for good governance and this statement describes how the

relevant principles of governance are applied to the Group. Throughout the year ended June 30, 2006, the Company has been in compliance with the code provisions set out in Section 1 of the Combined Code on Corporate Governance issued by the Financial Reporting Council in July 2003 except for the following matters:

- ◊ The roles of Chairman and CEO are combined and undertaken by Sir Alan Sugar, which the Board considers is appropriate given the entrepreneurial nature and size of the Company.
- ◊ The Company does not have a separate Nominations Committee as the Board believes that given the size of both the Company and the Board, this role should be undertaken by the Board as a whole.
- ◊ The Board has adopted an informal approach to evaluating the individual performance of directors, Board Committees, and the Board as a whole and as such does not strictly comply with the Combined Code's requirement for a formal evaluation process.

The Board The Board is responsible to shareholders for the proper management of the Group. The matters specifically reserved for decision by the Board include:

- ◊ Setting and monitoring Group strategy
- ◊ Approving the annual budget and any major capital expenditure or divestment projects
- ◊ Reviewing trading performance during the year
- ◊ Reviewing the Group's systems of internal control and risk management
- ◊ Approving the terms of reference of Board Committees
- ◊ Approving appointments to the Board and the appointment of the Company Secretary
- ◊ Approving Directors' remuneration and the remuneration policy for the Company

The Board consists of five executive directors and two nonexecutive directors. On appointment to the Board, each new appointee is required to stand for election at the next Annual General Meeting following their appointment. In addition, one third of the Board retires by rotation at each Annual General Meeting with every director seeking reelection at least every three years. The names and responsibilities of individual directors are set out on page 1. Both nonexecutive directors are considered by the Board to be independent of management and free from any business or other relationship that could materially interfere with the exercise of independent judgment. The Board has designated Mr. J. E. Samson as the senior nonexecutive director. The terms and conditions of employment of the nonexecutive directors are available for inspection at

> the Company's registered office and at the Company's Annual General Meeting.
>
> The roles of Chairman and CEO are combined and undertaken by Sir Alan Sugar, which the Board considers appropriate given the entrepreneurial nature and size of the Company. Sir Alan Sugar is also a director of various companies within the Amshold group, which he controls.
>
> All directors are given full and free access to all relevant information and are able to take independent professional advice in the furtherance of their duties.
>
> The Company Secretary has the responsibility for ensuring Board procedures are followed and for advising on governance matters. The Company Secretary is also secretary to the Audit and Remuneration Committees. Formal minutes of Board and Committee meetings are prepared and distributed as appropriate to each director.

So we have another qualified corporate governance report. This time it is the role of the chief entrepreneur that is taken into account, together with a management approach that is more informal than that set out in the code. The question in this case is whether the disclosure actually adds anything to the reader's understanding of the company. Anyone knowing Amstrad knows that Alan M. Sugar is crucial to the development of the business and if they were to invest they are in many ways considering his likelihood of being successful. Yes, they have met most of the key elements of the code with a couple of exceptions, and yes again, the market will probably overlook these exceptions.

Indeed it is generally only when a company is failing that the market then looks to corporate governance procedures and starts to wag a disapproving finger. In the case of Morrisons, a UK supermarket chain, the failure to comply with corporate governance standards was not considered a problem until such time as the market became dissatisfied with corporate performance. Changes were requested and made and performance has begun to improve—but would the same performance improvement have occurred with or without a corporate governance code? Of course we shall never know, but the evidence of out performance of companies with good corporate governance is generally considered to be rather patchy.

(c) ACCOUNTING/FINANCE ENVIRONMENT. With the advent of International Accounting Standards, including the much-maligned IAS 39 on measurement of financial instruments, companies on a global basis should all be producing consistent accounts to enable global comparison. However, the extent to which the playing field is actually level is still open to conjecture.

The UK accounting and finance industry always embraces these new standards with vigor and tries to make them work. The problem is whether they actually improve the ability of senior management to meet their corporate governance obligations.

With the increasing use of capital accounting through reserves and increasingly arcane accounting and measurement techniques, there must be significant doubt that most directors are capable of interpreting their own accounts yet alone those of their competitors. As accounts increase in length and complexity the challenge is to maintain transparency and understanding. I have to say that in my opinion the current International Accounting Standards have become complex and in some cases at best unhelpful. The issue to be considered is who now really understands the accounts and what they mean. As we move further from historic cost accounting and increasingly seek to use reserves for nontrading movements there is certainly the risk that transparency is lost. With changing standards, comparative information is often difficult to obtain—and sometimes this is impossible. Standard credit and investment analysis techniques therefore become inoperable since they are actually tracking movements in accounting numbers, which may actually be due to changes in accounting standards, rather than changes in the underlying business.

That being said, the UK finance profession fully understands the stewardship role and fiduciary responsibilities that exist. With a largely qualified profession of high-quality specialists, the presence of the relevant institutes adds additional credence to the role of finance in governance. There is an in-depth understanding of ethical standards and the ethical easy of doing business ingrained within the UK accountancy professions. This often means that wrongdoing, where it occurs, is often identified within the companies' own finance function. This is combined with most firms having also implemented whistle-blowing charters, although there is still the residual concern that nobody will actually hire a whistle-blower.

When corporate governance goes wrong it is often the finance function that is in the best position to identify that there is wrongdoing. They are in a much better position than either internal or external audit since those functions at best can only view issues periodically. With their ingrained ethical standards, UK chartered accountants in industry effectively act as the watchdogs of the corporate governance code.

(d) AUDITING ENVIRONMENT. The UK auditing environment falls into two separate areas:

- Internal audit
- External audit

The increasing prominence of the internal audit functions in major companies is to be welcomed. Clearly they have a role in corporate governance and reporting lines to both the chairman and the audit committee, where such a committee exists. This enables them to look at the key values of the company and the primary responsibilities of the board and to ensure that these are met.

Of course the role of the internal audit function should go much further than that. They are no longer a tick-box function seeking to hammer failures that are in effect inconsequential and result in expensive controls being implemented that themselves detract value. Rather they are akin to an internal consultancy function seeking to improve the business of their company.

Maintaining an adequately trained and independent internal audit function is crucial to the ongoing corporate governance of a firm. Without such a function there is nobody checking that actions are actually delivered.

External audit is in a different position. Current UK audit reports typically look like this:

> GlaxoSmithKline plc 2005 Independent Auditors' Report (extract)
>
> We review whether the Corporate Governance Statement reflects the company's compliance with the nine provisions of the 2003 FRC Combined Code specified for our review by the Listing Rules of the Financial Services Authority, and we report if it does not. We are not required to consider whether the board's statements on internal control cover all risks and controls, or form an opinion on the effectiveness of the group's corporate governance procedures or its risk and control procedures.

So the external auditors have a limited brief in this respect. Since they do not mention a qualification in the report, the assumption must be that the nine key components of the Combined Code have in fact been complied with.

64.2 COMPLIANCE TRENDS: CHALLENGES AND OPPORTUNITIES

(a) CULTURAL AND POLITICAL. The trends in corporate governance mirror changes that are actually also occurring within compliance in general. For larger firms, compliance has become a major industry and one in which the UK could be seen to be leading. While financial services are the obvious candidate for consideration, such regulation is all-embracing with any industry that has a public interest being affected.

Even smaller companies that are not required to comply with Listed Company rules are likely to be affected. Such regulations affect the amount of time a person may work, the recruitment of minorities or the disabled, the retirement of individuals, their pensions provision, the workplace in which they work, and the provision of certain benefits. Effectively, legislation and regulation, and specifically the UK implementation of European legislation, are embedded throughout business.

The UK approach of offering general guidance can often be at odds with the European approach for detail. In the UK the main approach has been that everything is fine unless a regulation says it is not. The other approach in Europe is that everything is illegal unless it is specifically permitted. This conundrum often lies at the heart of discussions in the UK and highlights why it is so important for UK firms to follow European regulatory developments.

(b) LEGAL. The legal challenge for a large company is that the regulations often conflict with each other. Simple cases such as the conflicts between money-laundering deterrence legislation and data protection regulations are well documented, but not isolated cases. The impact of each regulation on the myriad of other relevant corporate statutes and guidance can cause many problems for a major firm and are often ignored altogether by smaller firms.

(c) TECHNOLOGY. Increasingly firms are resorting to technology to enable them to demonstrate to their boards and regulators that they are complying with the relevant rules and regulations. Whether this is in the form of control and risk self-assessment software or gap analysis software, such tools enable the board to obtain a view of their compliance with relevant rules and regulations.

The software is not generally expensive—perhaps £300,000 for a moderate-sized company, or perhaps even a rental charge. However, the amount of management time that is required to properly embed such a product into the corporate structure should not be underestimated and is likely to be a multiple of the software cost.

(d) PROCESS. The process is easy. Identify all of the regulations to which your firm should comply and then ensure that each regulation is owned. Then consider what the loss to the firm would be from noncompliance and also review the relevant controls that ensure compliance. As the rules change so must the control procedures operated by the company change to meet these new requirements.

Easy to say, but difficult to achieve. The quality of process modeling maintained within firms has definitely slipped over recent years and for many companies reinventing such process maps has been a lengthy task. Again, software modeling solutions are available and commonplace, but it is the management effort that is crucial in such cases.

(e) PEOPLE. One of the consequences of the rise in compliance requirements has been on the salaries of compliance professionals. Originally such requirements were often just within the human resources arena, but now they are recognized as a separate subject on their own.

The development of specialist bodies dealing explicitly with compliance is the response of the industry to the need that has been identified. Compliance professionals are now an in-demand commodity within business generally and their cost is rising as the risks that they manage continue to increase.

64.3 THE MARKET AND HUMAN BENEFITS OF GETTING THERE SOONER RATHER THAN LATER

We would normally recommend that a firm should not be ahead of its peers in implementing and rule or regulation. The reason for this is simple. The UK has seen a number of cases where rules and regulations were nearly implemented only for their actual implementation to actually be canceled. Perhaps the worst

case of this recently was the 2005 cancellation of the Operating and Financial Review (OFR).

The OFR was the first real attempt to bring together risk information in a holistic manner—effectively how it is looked at within a business. Its cancellation just months before it was due to be compulsory for listed companies caused great concern.

We would recommend that any firm should look to follow the pack in such areas, complying with clear principles but waiting for actual guidance to emerge prior to spending large amounts of time that may ultimately prove to be futile.

64.4 CONCLUSION

Corporate governance standards are well embedded within UK business and generally well served by the accounting and legal professions. However there remains a risk that another corporate governance failure will appear with people being disadvantaged since it is always the scrupulous that comply with rules and the unscrupulous that fail to do so.

CHAPTER 65

UNITED KINGDOM'S COMBINED CODE

Anthony Tarantino, PhD

65.1 INTRODUCTION

Companies incorporated in the UK and listed on the UK stock exchange are subject to the Combined Code. The 2003 version combines the Greenbury and Cadbury Reports on corporate governance, the Smith Guidance on audit committees, the Turnbull Guidance covering internal controls, plus some elements of the Higgs Report.

The Financial Aspects of Corporate Governance is better known as the Cadbury Report of 1992 because the committee was chaired by Adrian Cadbury. Cadbury was a director of the Bank of England and IBM, as well as a member of the Organization for Economic Cooperation and Development's (OECD) Business Sector Advisory Group on Corporate Governance. The Cadbury Report was truly pioneering in its guidance on the organization and activities of corporate boards, and has been accepted as a role model by many nations or organizations. The Combined Code owes much to Cadbury and the commission he championed many years before corporate governance became such a major issue throughout the world.

The Combined Code follows a "comply or explain" basis, in which companies may choose not to comply with a specific provision but are then required to provide a public statement explaining their reasons for not complying.

65.2 BOARD OF DIRECTORS

The following is a summary of the Combined Code's "Code of Best Practices."[1]

- Every company should be headed by an effective board, which is collectively responsible for the success of the company.
- The board's role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls, which enables risk to be assessed and managed.
- The board should set the company's strategic aims, ensure that the necessary financial and human resources are in place for the company to meet its objectives, and review management performance.
- The board should set the company's values and standards and ensure that its obligations to its shareholders and others are understood and met.
- All directors must take decisions objectively in the interests of the company.
- As part of their role as members of a unitary board, nonexecutive directors should constructively challenge and help develop proposals on strategy.
- Nonexecutive directors should scrutinize the performance of management in meeting agreed goals and objectives and monitor the reporting of performance. They should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust and defensible. They are responsible for determining appropriate levels of remuneration of executive directors and have a prime role in appointing, and where necessary removing, executive directors, and in succession planning.
- The board should meet sufficiently regularly to discharge its duties effectively. There should be a formal schedule of matters specifically reserved for its decision.
- The annual report should include a statement of how the board operates, including a high level statement of which types of decisions are to be taken by the board and which are to be delegated to management.
- The annual report should identify the chairperson, the deputy chairperson (where there is one), the chief executive, the senior independent director, and the chairmen and members of the nomination, audit, and remuneration committees.
- The annual report should also set out the number of meetings of the board and those committees and individual attendance by directors.
- The chairperson should hold meetings with the nonexecutive directors without the executives present.
- Led by the senior independent director, the nonexecutive directors should meet without the chairperson present at least annually to appraise the chairperson's performance and on such other occasions as are deemed appropriate.

- Where directors have concerns which cannot be resolved about the running of the company or a proposed action, they should ensure that their concerns are recorded in the board minutes.
- On resignation, a nonexecutive director should provide a written statement to the chairperson, for circulation to the board if they have any such concerns.
- The company should arrange appropriate insurance cover in respect of legal action against its directors.

65.3 CHAIRPERSON AND CHIEF EXECUTIVE

The following is a summary of the roles and responsibilities of the chairperson of the board (COB) and chief executive officer (CEO):

- There should be a clear division of responsibilities at the head of the company between the running of the board and the executive responsibility for the running of the company's business.
- No one individual should have unfettered powers of decision.
- The chairperson is responsible for leadership of the board, ensuring its effectiveness on all aspects of its role and setting its agenda.
- The chairperson is also responsible for ensuring that the directors receive accurate, timely, and clear information.
- The chairperson should ensure effective communication with shareholders. The chairperson should also facilitate the effective contribution of nonexecutive directors in particular and ensure constructive relations between executive and nonexecutive directors.
- The roles of chairperson and chief executive should not be exercised by the same individual.
- The division of responsibilities between the chairperson and chief executive should be clearly established, set out in writing, and agreed to by the board.
- The chairperson should on appointment meet the independence criteria set out in a later section.
- A chief executive should not go on to be chairperson of the same company. If exceptionally a board decides that a chief executive should become chairperson, the board should consult major shareholders in advance and should set out its reasons to shareholders at the time of the appointment and in the next annual report.

65.4 BOARD BALANCE AND INDEPENDENCE

The Combined Code provides the following guidelines for board size, composition, organization, and independence:

- The board should include a balance of executive and nonexecutive directors (and in particular independent nonexecutive directors) such that no

individual or small group of individuals can dominate the board's decision making.

- The board should not be so large as to be unwieldy. The board should be of sufficient size that the balance of skills and experience is appropriate for the requirements of the business and that changes to the board's composition can be managed without undue disruption.
- To ensure that power and information are not concentrated in one or two individuals, there should be a strong presence on the board of both executive and nonexecutive directors.
- The value of ensuring that committee membership is refreshed and that undue reliance is not placed on particular individuals should be taken into account in deciding chairmanship and membership of committees.
- No one other than the committee chairperson and members is entitled to be present at a meeting of the nomination, audit, or remuneration committee, but others may attend at the invitation of the committee.
- The board should identify in the annual report each nonexecutive director it considers to be independent.
- The board should determine whether the director is independent in character and judgment and whether there are relationships or circumstances which are likely to affect, or could appear to affect, the director's judgment.
- The board should state its reasons if it determines that a director is independent notwithstanding the existence of relationships or circumstances which may appear relevant to its determination, including if the director:
    - Has been an employee of the company or group within the past five years
    - Has, or has had within the past three years, a material business relationship with the company either directly or as a partner, shareholder, director, or senior employee of a body that has such a relationship with the company
    - Has received or receives additional remuneration from the company apart from a director's fee, participates in the company's share option or a performance-related pay scheme, or is a member of the company's pension scheme
    - Has close family ties with any of the company's advisers, directors, or senior employees
    - Holds cross-directorships or has significant links with other directors through involvement in other companies or bodies
    - Represents a significant shareholder
    - Has served on the board for more than nine years from the date of his/her first election
- Except for smaller companies, at least half the board, excluding the chairperson, should comprise nonexecutive directors determined by the board to

be independent. A smaller company should have at least two independent nonexecutive directors.

- The board should appoint one of the independent nonexecutive directors to be the senior independent director. The senior independent director should be available to shareholders if they have concerns that contact through the normal channels of chairperson, chief executive, or finance director has failed to resolve or for which such contact is inappropriate.

65.5 APPOINTMENTS TO THE BOARD

The Combined Code provides the following guidelines around nominations and appointments:

- There should be a formal, rigorous, and transparent procedure for the appointment of new directors to the board.
- Appointments to the board should be made on merit and against objective criteria. Care should be taken to ensure that appointees have enough time available to devote to the job. This is particularly important in the case of chairmanships.
- The board should satisfy itself that plans are in place for orderly succession for appointments to the board and to senior management, so as to maintain an appropriate balance of skills and experience within the company and on the board.
- There should be a nomination committee who should lead the process for board appointments and make recommendations to the board.
- A majority of members of the nomination committee should be independent nonexecutive directors. The chairperson or an independent nonexecutive director should chair the committee, but the chairperson should not chair the nomination committee when it is dealing with the appointment of a successor to the chairmanship.
- The nomination committee should make available its terms of reference, explaining its role and the authority delegated to it by the board.
- The nomination committee should evaluate the balance of skills, knowledge, and experience on the board and, in the light of this evaluation, prepare a description of the role and capabilities required for a particular appointment.
- For the appointment of a chairperson, the nomination committee should prepare a job specification, including an assessment of the time commitment expected, recognizing the need for availability in the event of crises.
- A chairperson's other significant commitments should be disclosed to the board before appointment and included in the annual report. Changes to such commitments should be reported to the board as they arise, and included in the next annual report.
- No individual should be appointed to a second chairmanship of another publicly listed company.

- The requirement to make the information available would be met by making it available on request and by including the information on the company's web site. Compliance or otherwise with this provision need only be reported for the year in which the appointment is made.
- The terms and conditions of appointment of nonexecutive directors should be made available for inspection. The letter of appointment should set out the expected time commitment. Nonexecutive directors should undertake that they will have sufficient time to meet what is expected of them. Their other significant commitments should be disclosed to the board before appointment, with a broad indication of the time involved and the board should be informed of subsequent changes.
- The board should not agree to a full-time executive director taking on more than one nonexecutive directorship in another publicly listed company nor the chairmanship of such a company.
- A separate section of the annual report should describe the work of the nomination committee, including the process it has used in relation to board appointments. An explanation should be given if neither an external search consultancy nor open advertising has been used in the appointment of a chairperson or a nonexecutive director.

65.6 INFORMATION AND PROFESSIONAL DEVELOPMENT

The Combined Code provides the following guidelines regarding information, training, and counseling required by the board:

- The board should be supplied in a timely manner with information in a form and of a quality appropriate to enable it to discharge its duties.
- All directors should receive induction on joining the board and should regularly update and refresh their skills and knowledge.
- The chairperson is responsible for ensuring that the directors receive accurate, timely, and clear information. Management has an obligation to provide such information but directors should seek clarification or amplification where necessary.
- The chairperson should ensure that the directors continually update their skills and the knowledge and familiarity with the company required to fulfill their role both on the board and on board committees.
- The company should provide the necessary resources for developing and updating its directors' knowledge and capabilities. Under the direction of the chairperson, the company secretary's responsibilities include ensuring good information flows within the board.
- The company secretary should be responsible for advising the board through the chairperson on all governance matters.
- The chairperson should ensure that new directors receive a full, formal, and tailored induction on joining the board. As part of this, the company should

offer to major shareholders the opportunity to meet a new nonexecutive director.
- The board should ensure that directors, especially nonexecutive directors, have access to independent professional advice at the company's expense where they judge it necessary to discharge their responsibilities as directors.
- Committees should be provided with sufficient resources to undertake their duties.
- All directors should have access to the advice and services of the company secretary, who is responsible to the board for ensuring that board procedures are complied with.
- Both the appointment and removal of the company secretary should be a matter for the board as a whole.

65.7 PERFORMANCE EVALUATION

The Combined Code provides the following guidelines over the performance of board in general, individual directors, and board committees:

- The board should undertake a formal and rigorous annual evaluation of its own performance and that of its committees and individual directors.
- Individual evaluation should aim to show whether each director continues to contribute effectively and to demonstrate commitment to the role (including commitment of time for board and committee meetings and any other duties).
- The chairperson should act on the results of the performance evaluation by recognizing the strengths and addressing the weaknesses of the board and, where appropriate, proposing new members be appointed to the board or seeking the resignation of directors.
- The board should state in the annual report how performance evaluation of the board, its committees, and its individual directors has been conducted.
- The nonexecutive directors, led by the senior independent director, should be responsible for performance evaluation of the chairperson, taking into account the views of executive directors.

65.8 REELECTION

The Combined Code provides the following guidelines over the election and reelection of board directors:

- All directors should be submitted for reelection at regular intervals, subject to continued satisfactory performance. The board should ensure planned and progressive refreshing of the board.
- All directors should be subject to election by shareholders at the first annual general meeting after their appointment, and to reelection thereafter at intervals of no more than three years.

- The names of directors submitted for election or reelection should be accompanied by sufficient biographical details and any other relevant information to enable shareholders to take an informed decision on their election.
- The board should set out to shareholders in the papers accompanying a resolution to elect a nonexecutive director why they believe an individual should be elected.
- The chairperson should confirm to shareholders when proposing reelection that, following formal performance evaluation, the individual's performance continues to be effective and to demonstrate commitment to the role.
- Any term beyond six years (e.g. two three-year terms) for a nonexecutive director should be subject to particularly rigorous review, and should take into account the need for progressive refreshing of the board.
- Nonexecutive directors may serve longer than nine years (e.g., three three-year terms), subject to annual reelection. Serving more than nine years could be relevant to the determination of a nonexecutive director's independence.

65.9 FINANCIAL REPORTING

The Combined Code provides the following guidelines regarding financial reporting presented by the board, including requirements for sound internal controls and transparency

- The board should present a balanced and understandable assessment of the company's position and prospects.
- The board's responsibility to present a balanced and understandable assessment extends to interim and other price-sensitive public reports and reports to regulators as well as to information required to be presented by statutory requirements.
- The directors should explain in the annual report their responsibility for preparing the accounts and there should be a statement by the auditors about their reporting responsibilities.
- The directors should report that the business is a going concern, with supporting assumptions or qualifications as necessary.

Internal Control

- The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.
- The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so.
- The review of internal controls should cover all material controls, including financial, operational, and compliance controls and risk management systems.

65.10 AUDIT COMMITTEE AND AUDITORS

The Combined Code provides the following guidelines regarding audit committee composition, organization, and charter and its relationship with external auditors

- The board should establish formal and transparent arrangements for considering how they should apply the financial reporting and internal control principles and for maintaining an appropriate relationship with the company's auditors.
- The board should establish an audit committee of at least three, or in the case of smaller companies two, members, who should all be independent nonexecutive directors. The board should satisfy itself that at least one member of the audit committee has recent and relevant financial experience.
- The main role and responsibilities of the audit committee should be set out in written terms of reference and should include:
  - To monitor the integrity of the financial statements of the company, and any formal announcements relating to the company's financial performance, reviewing significant financial reporting judgments contained in them
  - To review the company's internal financial controls and, unless expressly addressed by a separate board risk committee composed of independent directors, or by the board itself, to review the company's internal control and risk management systems
  - To monitor and review the effectiveness of the company's internal audit function
  - To make recommendations to the board, forward it to shareholders for their approval in a general meeting, in relation to the appointment, reappointment and removal of the external auditor and to approve the remuneration and terms of engagement of the external auditor
  - To review and monitor the external auditor's independence and objectivity and the effectiveness of the audit process, taking into consideration relevant local/national professional and regulatory require ments
  - To develop and implement policy on the engagement of the external auditor to supply nonaudit services, taking into account relevant ethical guidance regarding the provision of nonaudit services by the external audit firm; and to report to the board, identifying any matters in respect of which it considers that action or improvement is needed and making recommendations as to the steps to be taken
- The terms of reference of the audit committee, including its role and the authority delegated to it by the board, should be made available. A separate section of the annual report should describe the work of the committee in discharging those responsibilities.

- The audit committee should review arrangements by which staff of the company may, in confidence, raise concerns about possible improprieties in matters of financial reporting or other matters. The audit committee's objective should be to ensure that arrangements are in place for the proportionate and independent investigation of such matters and for appropriate follow-up action.
- The audit committee should monitor and review the effectiveness of the internal audit activities. Where there is no internal audit function, the audit committee should consider annually whether there is a need for an internal audit function and make a recommendation to the board, and the reasons for the absence of such a function should be explained in the relevant section of the annual report.
- The audit committee should have primary responsibility for making a recommendation on the appointment, reappointment and removal of the external auditors. If the board does not accept the audit committee's recommendation, it should include in the annual report, and in any papers recommending appointment or reappointment, a statement from the audit committee explaining the recommendation and should set out reasons why the board has taken a different position.
- The annual report should explain to shareholders how, if the auditor provides nonaudit services, auditor objectivity and independence are safeguarded.

65.11 SUMMARY

While the Combined Code practices make good sense and are advocated by most champions of good governance, there are no guarantees. The Combined Code advocates greater board independence and financial expertise, yet some of the worst cases of corporate fraud occurred in companies with a high ratio of outside directors—Tyco, 65 percent; WorldCom, 45 percent; and Enron, 80 percent. Many of these firms also had audit committees chaired by well-respected lawyers, bankers, and accountants.[2]

Notes

1. The Combined Code on Corporate Governance, July 2003, www.fsa.gov.uk/pubs/ukla/lr_comcode2003.pdf.
2. Margit Osterlo and Bruno S. Frey, "Corporate Governance for Crook? The Case for Corporate Virtue," Working Paper 2005-10, Center for Research in Economics, Management and the Arts.

CHAPTER 66

CORPORATE GOVERNANCE: UNITED STATES

Anthony Tarantino, PhD

66.1 THE U.S. CORPORATE GOVERNANCE MODEL

The Federal System. In most nations, the central government has primary responsibility over corporations. The U.S. federal system is different with the 50 individual states possessing primary responsibility over corporate law. This translates into 50 flavors of corporate and security (blue sky) laws, regulatory agencies, and court systems. More than half of major corporations are incorporated in the state of Delaware. This is because of its business-friendly corporate legal environment and its state court dedicated to resolving business issues. Most states, but not Delaware, follow the American Bar Association's Model Business Corporation Act. On a national level, the Securities and Exchange Commission (SEC) and federal courts are charged with enforcing federal laws and regulations. This variety of regulations has not hampered the United States in attracting global capital and provides a degree of checks and balances not found in other systems. The most visible manifestation of this has been the aggressive prosecution of corporate wrongdoing

by New York State's attorney general, Eliot Spitzer, who used his success in the courtroom as the foundation for his successful quest for the governorship.[1]

The Shared Vision of Corporate Governance. The United States, European Union, and other leading economies share a vision of corporate governance as the method in which companies assure investors and other stakeholders (customers, suppliers, community, regulators, rating agencies) that they are utilizing assets in an appropriate manner to foster profitability and growth. They also share a belief that good corporate governance, political and financial stability, and the rule of law will improve investor confidence and attract global capital, resulting in premium stock prices in the marketplace. They also share a belief that failures in governance, political and financial stability, and the rule of law will reduce investment and ultimately hurt economic prosperity.

The United States, like many markets, has experienced periodic pendulum swings between a laissez-faire approach to governance in which governance took a backseat until scandals shook confidence and swung the pendulum toward greater oversight and controls. Unfortunately, the pendulum tends to swing too far in both directions. The dot-com boom of the 1990s witnessed a period in which common sense was lacking and get-rich-quick schemes overwhelmed ethical and fair behavior. This was followed by a period of very strong regulation with the enactment of the Sarbanes-Oxley Act and a renewed emphasis of corporate governance.

The U.S. Model of Corporate Governance. Holly G. Gregory, a leading authority in corporate governance has helped organize corporate governance programs for the Organization for Economic Cooperation and Development (OECD), the World Bank, the Global Corporate Governance Forum, Yale's International Institute for Corporate Governance, Transparency International, the SEC, and Columbia University School of Law's Institutional Investor Project. Ms. Gregory provides the following insights into the common and unique aspects of U.S. corporate governance:

- *Board responsibilities.* In the United States and most countries, "the board is responsible for the corporation's stewardship and has responsibilities which are separate and distinct from management's responsibilities. There is a general agreement that board functions will include the selection, oversight, compensation, and termination of senior management. The board will also provide oversight of the corporation's performance and related functions of strategic planning and risk and management, succession planning, shareholder communication, financial disclosure oversight and internal controls (critical in the US with Section 404 of the Sarbanes Oxley Act), and the oversight of general adherence to laws and regulations.
- *Board composition.* Laws, regulations, or listing rules often contain requirements regarding board composition. As an example, publicly traded companies in the United States are required by NASDAQ and New York Stock Exchange (NYSE) to contain a majority of independent board directors, and

audit committees must have one or more members who meet certain requirements related to financial expertise.

- *Director nomination.* The process of directors' nominations is also subject to disclosure and listing regulations, with NASDAQ and NYSE corporations mandated to place this responsibility with independent directors.
- *Independence.* "It is essential that directors are able to exercise objective judgment over management's performance. Without it, they can not play a significant oversight role. For this reason, the independence of directors has become an important issue in much of the world. In the United States, the listing requirements of major exchanges mandate a majority of directors be free of material relationships with the company and its senior management team. Best practice documents such as UK's Cadbury Report and America's National Association of Corporate Directors Report on Director Professionalism "view the ultimate determination of just what constitutes 'independence' to be an issue for the board itself to determine. The New York Stock Exchange prohibits a board from finding a director to be independent if any of the relationships described above are present, but also places an affirmative obligation on the board to consider whether other relationships might impair independence." Independent board leadership is a key element in many codes of best practice reflecting a developing understanding that if a board is to be a distinct oversight body, it needs leadership distinct from the executive team. As explained by the National Association of Corporate Directors (U.S.): "The purpose of creating [an independent] leader is not to add another layer of power but . . . to ensure organization of, and accountability for, the thoughtful execution of certain critical independent functions"—such as evaluating the CEO, chairing sessions of the nonexecutive directors, setting the board agenda, and leading the board in responding to crisis. Jurisdictions outside the United States that place less emphasis on the importance of independent directors tend to rely on the importance of separating the roles of chairman and CEO.[2]

66.2 U.S. REGULATORY AGENCIES AND REGULATIONS OF INTEREST

The Securities and Exchange Commission. This is a very short introduction to the regulatory charter and organization of the SEC.

- The mission of the SEC is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.
- To achieve this, the SEC requires public companies to disclose meaningful financial and other information to the public. This provides a common pool of knowledge for all investors to use to judge for themselves whether to buy, sell, or hold a particular security.
- Only through the steady flow of timely, comprehensive, and accurate information can people make sound investment decisions.

- The SEC oversees the key participants in the securities world, including securities exchanges, securities brokers and dealers, investment advisers, and mutual funds. Here the SEC is concerned primarily with promoting the disclosure of important market-related information, maintaining fair dealing, and protecting against fraud.
- Each year the SEC brings hundreds of civil enforcement actions against individuals and companies for violation of the securities laws.
- Typical infractions include insider trading, accounting fraud, and providing false or misleading information about securities and the companies that issue them.

Sarbanes-Oxley Act (SOX, SOA, Sarbox) of 2002. The act consists of several sections which are designed to improve internal controls, as well as executive and auditor accountability. Most of the changes were so fundamental to sound governance that it is disappointing that major scandals were needed to spur reforms.

- **Section 201—Audit Firm Conflict of Interest, No Consulting Except Tax.** Auditing services were not seen as lucrative so there was strong pressure on audit firms to use audit insights to sell lucrative consulting services. Section 201 helped to resolve an obvious conflict of interest which the audit firms were incapable of addressing through self regulation.
- **Section 203—Five-Year Rotation of Audit Firms.** Rotating audit firms on a periodic basis is good practice that will keep auditors and their clients on their toes. Without the rotation, audit firms can become complacent and lack the vigilance to thoroughly examine their clients.
- **Section 204—Auditor Reports to Audit Committee of Board.** This was an essential reform to assure that auditor findings, good and bad, were not buried at lower levels of an organization
- **Section 206—CXO Conflict of Interest, One Year Removed from Audit Firm.** This removed a common and unwise practice of auditors jumping to their clients.
- **Section 302—CEO and CFO Liable for Certifying Financial Results.** This is one of most dramatic changes in corporate governance. CEOs and CFOs could no longer play a passive role in financial results. Under Section 302 they must take ownership to the work of their subordinates. Ignorance was no longer a valid excuse.
- **Section 306—No Insider Trading During Blackout Period.** This is another much-needed reform to prevent executives from trading shares based on insider information not available to other shareholders.
- **Section 401—Off-Balance-Sheet (OBS) Obligations and Special Purpose Entities (SPEs).** This section can be attributed to the very clever accounting tricks that Enron deployed to hide financial losses. In the *Manager's Guide to Compliance*, we dedicate a chapter to describing the

complexities in the process even after the enactment of Section 401 that leave open the opportunities for confusion, errors, and fraud. These problems can only be resolved by an overhaul of the U.S. Tax Code.

- **Section 402—No Personal Loans to Executives.** This was yet another abuse that needed to end.
- **Section 403—48-Hour Notice of Executive Stock Transactions.** This section did not appear to be such a big deal back in 2002, but in hindsight may be one of the wisest decisions of regulators. It ended the practice of companies backdating stock options. Before Section 403, companies did not have to declare option grants for weeks or even months after the fact. This opened the opportunity for widespread abuse as companies would pick an optimum date in the past as the date the options were granted. The practice is not inherently illegal, but the abuse came in understating the costs of stock options. (See Chapter 8 for a more detailed discussion on stock options.)
- **Section 404—Internal Control Attestation.** This is the most controversial provision of the act. Everyone agrees that robust internal controls are important and improve the accuracy of financial controls. The controversy comes in how audit firms have interpreted the act and the companion Audit Standard Number 2 (AS2). AS2 was issued by the Public Company Accounting Oversight Board (PCAOB), which was created as part of SOX to oversee audit firms. After the collapse of Arthur Andersen as a result of the Enron fiasco, audit firms became very risk averse and tended to err on the side of overly strict auditing. The old 5 percent rule, in which auditors did not focus on problems with a minor financial impact, was replaced with a very aggressive approach that examined all controls, no matter how minor their financial impact. The impact of Section 404 on small to mid-size companies has been a major issue as well, with three years' worth of promised relief to yet produce any tangible results.
- **Section 409—Real-Time Disclosure of Material Changes.** Section 409 requires the timely notification of material events, which were greatly expanded. The reporting is via the existing 8-K Form.
- **Section 806—Whistle-Blower Protection.** Historically, corruption is uncovered by whistle-blowers and not from external auditors, internal auditors, or regulators. Section 806 provides needed protection for whistle-blowers and also removes excuses for remaining silent when fraud is detected.
- **Title VIII and Title IV—Five-Year Data Retention by Auditors and Hard Jail Time.** The new regulations require auditors to retain every scrap of paper involved in their audits of clients. This was a result of Arthur Andersen's action in the Enron scandal, in which audit documents were intentionally destroyed in the face of regulatory investigations. The one-count conviction of the firm, eventually overturned on appeal, destroyed the most

prestigious and largest audit firm in the world. Enron and other scandals also changed America's attitude toward white-collar crimes. With the loss of thousands of jobs and billions of dollars in shareholder value, white-collar criminals were now seen as bad guys who needed to be punished as much as common or blue-collar criminals.

Section 401 Detail. The SEC has defined the term *off balance sheet (OBS) arrangement* as:

> "any transaction, agreement, or other contractual arrangement to which an entity that is not consolidated with the company is a party, under which the company, whether or not a party to the arrangement, has, or in the future may have:
>
> - Any obligation under a direct or indirect guarantee or similar arrangement,
> - A retained or contingent interest in assets transferred to an unconsolidated entity or similar arrangement,
> - Derivatives, to the extent that the fair value thereof is not fully reflected as a liability or asset in the financial statements, and
> - Any obligation or liability, including a contingent obligation or liability, to the extent that it is not fully reflected in the financial statements (excluding the footnotes thereto)."

Section 401 Requirements. Section 401 requires:

- The listing of off-balance-sheet (OBS) arrangements, transactions, and obligations (including contingent obligations) that may have a material effect, current or future, on:
  - Financial conditions
  - Changes in financial results in operations
  - Liquidity capital expenditures
  - Capital resources
  - Significant components
  - Revenues
  - Expenses
- The disclosure of "the nature and business purpose of the OBS arrangements, why and how they are needed in running a business." The Enron scandal was based on OBS abuses. Problems persist in the complexity and resulting confusion in how to account for OBS arrangements. Unfortunately, the SEC has not simplified the process to the extent to preclude significant abuse.

Section 404 Chronology. The thrust to improve internal controls is not new in U.S. corporate governance. The SEC has been promoting improvements for decades, but it took the scandals of the 1990s to bring the issue to a head.

- September 1977—Foreign Corrupt Practices Act is enacted into law requiring internal accounting controls.

- July 2002—Sarbanes-Oxley Act is signed into law, including Section 404.
- June 2003—SEC adopts rules and deadline for Section 404—11/15/04—for accelerated filers.
- September 2005—SEC postpones compliance date for nonaccelerated filers to 7/15/07.
- May 2006—SEC rejects its own elite committee recommendations to exempt smaller companies from the full force of Section 404.
- July 2006—SEC Concept Release on Section 404 asks for further discussion and promises small company relief from revised Committee of Sponsoring Organizations (COSO) guidance and revised Audit Standard No. 2 (AS2)—*mostly talk, little action, no teeth*.
- July 2006—COSO releases small company guidance at behest of SEC.
- November 2006—SEC agrees to reform Section 404 to reduce costs of compliance.
- February 2007—The PCAOB and SEC propose changes that would make the audit of internal controls more risk-based and top-down and receives hundreds of suggestions during the comment period.
- June 2007—The PCAOB releases a draft of AS5 for public comment.

Section 404 Detail. Section 404 has generated more discussion than all the other sections of Sarbanes-Oxley Act combined. For years many U.S. firms have neglected internal controls. They failed to follow the old adage of saying what you do and doing what you say. Oftentimes processes and their accompanying internal controls were poorly understood and documented and inconsistently applied across organizations. The major issues around the section include:

- Over the decades, the SEC has ruled that internal controls include policies, procedures, training programs, and other processes beyond financial controls.
- The SEC has defined internal controls to include "the safeguarding of assets against unauthorized acquisition, use, or disposition." Companies will need to document and test the adequacy of these internal process controls as well.
- The SEC has looked to the COSO for its understanding of internal controls. COSO's concept of internal controls is gaining acceptance as a global standard.
- According to COSO, internal control is a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - Effectiveness and efficiency of operations
    - Reliability of financial reporting
    - Compliance with applicable laws and regulations

- We argue in our COSO and operational risk chapters that the original COSO framework is outdated and that even its updated framework (Enterprise Risk Management) lacks a viable means to quantify, rationalize, and prioritize risk based on its likeliness, financial impact, and ability to be detected.

Section 409 Detail. Requires a "real-time issuer disclosure . . . on a rapid and current basis" or the reporting of material events, which affects financial reporting. "Timely" and "real-time" are defined as four days. An 8-K form via EDGAR is used for this process. The SEC describes EDGAR as follows: "For the past several years, the EDGAR electronic filing system has enabled domestic public companies to file their documents with the Commission from anywhere in the world within significantly shortened time frames. These documents are now available to the public through EDGAR on a real-time basis." The events requiring an 8-K form now include the following under Section 409:

- A change in control, a significant acquisition, or a bankruptcy
- Entry into a material agreement not made in the ordinary course of business
- Termination of a material agreement not made in the ordinary course of business
- Termination or reduction of a business relationship with a customer that constitutes a specified amount of the company's revenues
- Creation of a direct or contingent financial obligation material to the company
- Events triggering a direct or contingent financial obligation material to the company, including any default or acceleration of an obligation
- Exit activities including any material write-off or restructuring
- Any material impairment
- A change in a rating agency decision, issuance of a credit watch, or change in a company outlook
- Movement of the company's securities from one national securities exchange or interdealer quotation system of a registered national securities association to another, delisting of the company's securities from an exchange or quotation system, or a notice that a company does not comply with a listing standard
- Notice to the company from its currently or previously engaged independent accountant that the independent accountant is withdrawing a previously issued audit report or that the company may not rely on a previously issued audit report
- Any material limitation, restriction, or prohibition, including the beginning and end of lockout periods, regarding the company's employee benefit, retirement, and stock ownership plans

PCAOB and Audit Standard No. 2 Chronology.

The chronology of the PCAOB and its controversial Audit Standard No. 2 (AS2), which covers Section 404, can be summarized as follows:

- July 2002—PCAOB is created as part of Sarbanes-Oxley Act. The PCAOB conducts an annual review of all audit firms issuing over 100 audits per year, and once every three years for smaller audit firms.
- June 2004—SEC approves PCAOB's AS2.
- May 2006—PCAOB releases four-point plan to improve audit process, including guidelines for auditors to increase their use of the work done by others. This opens the door for companies to lower audit fees through greater use of compliance automation tools. Typically, auditors will audit manual controls much more extensively than automated controls. Companies can also reduce external audit fees through more robust internal audit efforts.
- November 2006—PCAOB agrees to rewrite AS2 to reduce the cost of compliance following years of broad-based criticism that the costs outweigh the benefits.
- February 2007—Comment period ends on proposed changes to AS2.

Proposed Replacement of AS2 with AS5. Responding the growing criticism of the Sarbanes-Oxley Act's Section 404, the SEC has proposed amendments to Exchange Act Rules 13a-15 and 15 d-15 that would allow a company that performs its evaluation in accordance with the interpretive guidance to have satisfied its annual evaluation requirements. The new guidance is "risk and materiality" focused and is intended make the evaluation of internal controls more efficient and effective. The SEC had not provided specific guidance for management in conducting its evaluation of internal control over financial reporting, forcing companies to rely on the PCAOB's AS2 and the COSO framework. The new Auditing Standard No. 5 is designed to allow companies to tailor evaluation methods fit their unique circumstances and characteristics. The SEC claims the new guidance is principles based and provides for a top-down, risk-based assessment of internal control over financial reporting, but in the next section, we will argue this is still not the case. The guidance focuses on the following two principles:

1. *Design of the controls.* Management should evaluate the design of the controls that it has implemented to determine whether there is a reasonable possibility that a material misstatement in the financial statements would not be prevented or detected in a timely manner.
2. *Operation of the controls.* Management should gather and analyze evidence about the operation of the controls being evaluated based on its assessment of the risk associated with those controls.

The SEC argues that these two principles will permit companies of all sizes and complexities to implement Section 404 more efficiently and effectively by focusing management on those controls needed to prevent or detect material misstatements in the financial statements. Unfortunately, it is difficult to see how this can be achieved without a means to quantify risks.

The proposal guidance covers four internal control areas:

1. *Identification of risks to reliable financial reporting* and the related controls that management has implemented to address those risks.
2. *Evaluation of operating effectiveness of controls*. The proposed guidance would provide a number of ways in which management may support its evaluation.
3. *Reporting the overall results of management's evaluation*. After conducting its evaluation, management must decide whether a control deficiency is a material weakness. The proposed guidance would provide a framework for this determination, outside of accounting literature, by describing the factors that management should consider to evaluate the severity of any deficiency.
4. *Documentation requirements*. The proposed guidance provides for flexibility in management's approach to documentation.

The SEC also proposed that the auditor's 404 report no longer include an opinion regarding management's evaluation of the effectiveness of internal controls, but only the auditor's own opinion regarding the effectiveness of internal controls.

Why the Proposed Changes to AS2 Fall Short. The Institute of Management Accountants (IMA) represents 65,000 accountants and financial professionals. The IMA describes management accountants as the "internal business-building role of accounting and finance professionals, who design, implement, manage, and report on internal accounting systems that support effective decision support, planning, and control over the organization's value-creating operations." The IMA issued a February 2007 evaluation of the PCAOB's proposed AS5 finding significant problems in the proposed audit standards and SEC regulations. The five major issues the IMA identified are:[3]

1. **Two Rule Books for the Same Task**—The SEC and PCAOB have not harmonized their tasks, which creates unneeded confusion and complexity. The SEC rules are higher-level while the PCAOB's are more detailed.
2. **Lack of a Top-Down and Risk-Based Approach**—The SEC's proposed rules and the PCAOB's revised standards are still not top-down or risk-based.
3. **Unrealistic Zero Defects Requirements**—The SEC and PCAOB have set the quality bar too high, calling for zero material defects.
4. **Perversion of Section 404**—The intent of Congress was for company management to assess their own internal controls and for external auditors to limit their activities to approving an independent report as to whether a company's management is taking its internal controls responsibilities

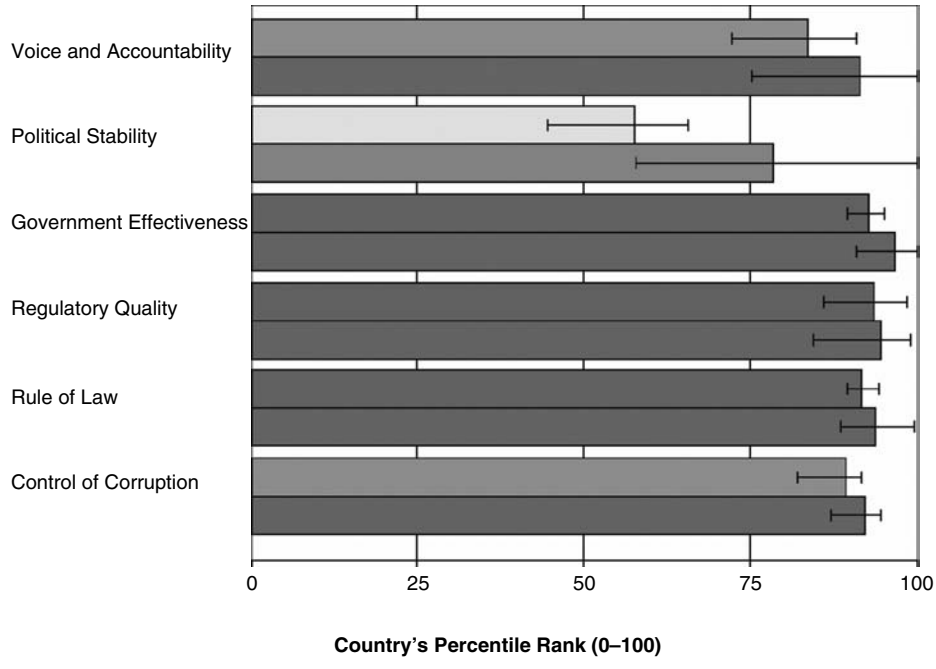
seriously and conscientiously. This is huge difference from the current practice in which auditors have doubled their revenue by auditing even the most insignificant controls and issuing their own view as to the effectiveness of controls.

5. **No Relief for the Little Guys—**In spite of continued rhetoric over the last four years by the SEC and PCAOB to provide support for small to mid size enterprises (SMEs), the only realistic solution for many smaller companies is to go private, merge, be acquired, or go out of business.

66.3 WORLD BANK RATINGS FOR SIX ELEMENTS OF GOVERNANCE

The World Bank publishes governance ratings for over 200 nations. The evaluation is based on six elements of governance. The latest ratings are for 2006 and represent one of the most viable means of comparing nations. The World Bank correctly assumes that corporate governance does not exist in a vacuum and can prosper only with factors that exist outside of corporations: political stability/lack of violence, government effectiveness, rule of law, corruption control, voice and accountably (freedom of religion, press, and speech), along with regulatory quality.

Exhibit 66.1 shows the World Bank percentile rank change from 2006 to 1996 (top-to-bottom order) for six elements of governance.[4]

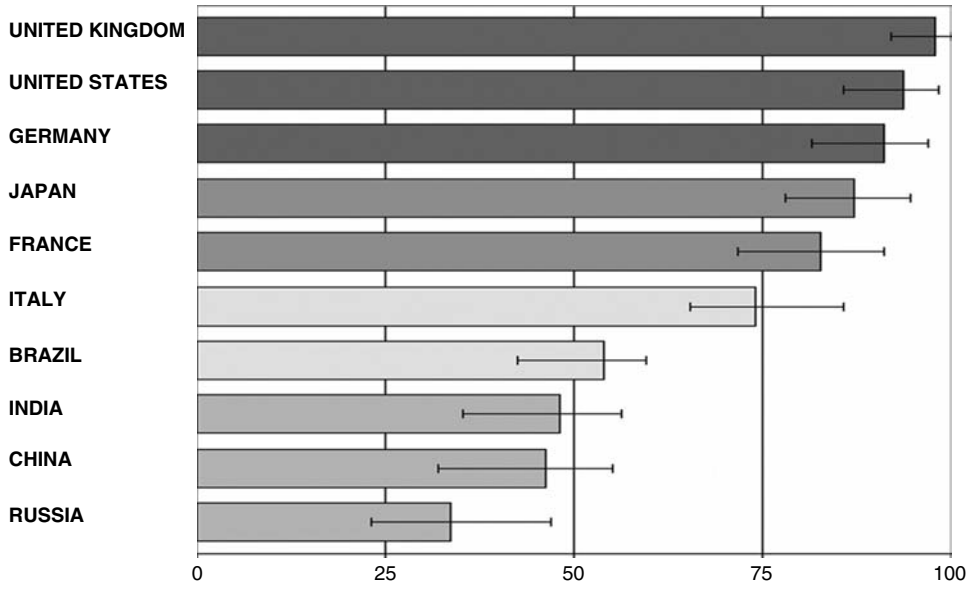


Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

EXHIBIT 66.1 THE WORLD BANK GOVERNANCE RANKINGS FOR THE UNITED STATES 2006 AND 1996 (TOP-TO-BOTTOM ORDER)

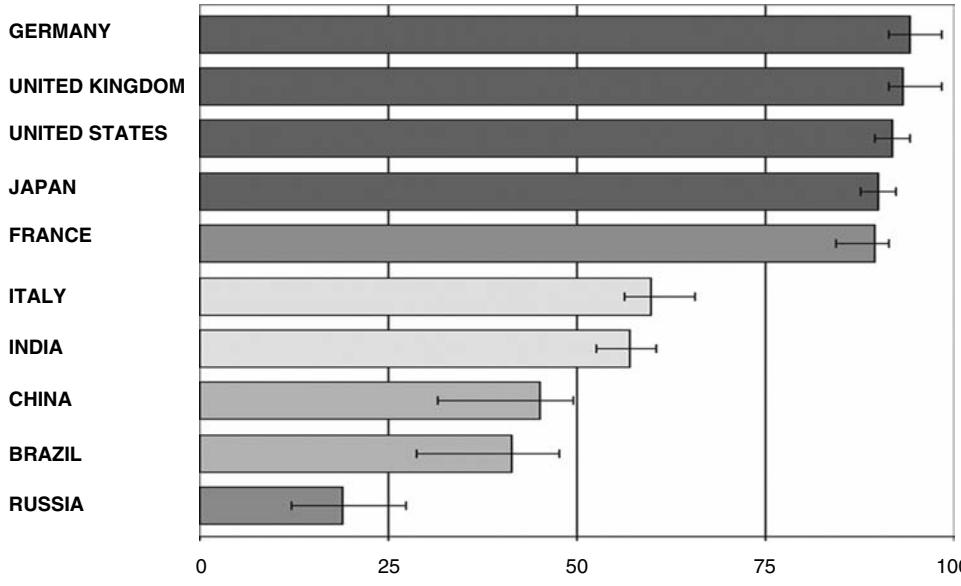
Regulatory Quality (2006)

The data on chart is sorted in descending order from top to bottom.



Rule of Law (2006)

The data on chart is sorted in descending order from top to bottom.



Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2006'' (World Bank, July 2007).

EXHIBIT 66.2 WORLD BANK GOVERNANCE RANKINGS: REGULATORY QUALITY AND RULE OF LAW FOR THE UNITED STATES AND MAJOR GDP COUNTRIES

In spite of the passage of the Sarbanes-Oxley Act and the high costs of complying with Section 404 as audited by the PCAOB's Audit Standard Number 2, the United States shows little improvement from 1996 even in the area of regulatory quality and the rule of law. In fairness, the United States ranks very well in regulatory quality and the rule of law when compared to the major GDP nations and the OECD. The World Bank statistics for 2005 are shown in Exhibit 66.2.[5]

Blame Canada and Maybe Australia as Well. Also of concern is the inability of the United States to rank any higher than fifth among the top GDP nations in World Bank governance ratings. We believe that the top-scoring nations have in common a stronger emphasis on board governance with the appropriate tone-at-the-top and principles approach over the U.S. rules-based bottom-up approach. It is ironic that the United States' neighbor to the north, with so many economic interdependencies with the United States, could be a great role model if American regulators would look beyond their borders for a solution. The United States has always had a strong bond with Australia as well, which ranks nearly as high as Canada. Canada and Australia share a corporate governance approach that has avoided the pain of a bottom-up approach with an overemphasis on rules. Instead, both nations have strong board governance regimes in place.[6] (See Exhibit 66.3.)

66.4 COMPETITIVENESS OF U.S. MARKETS

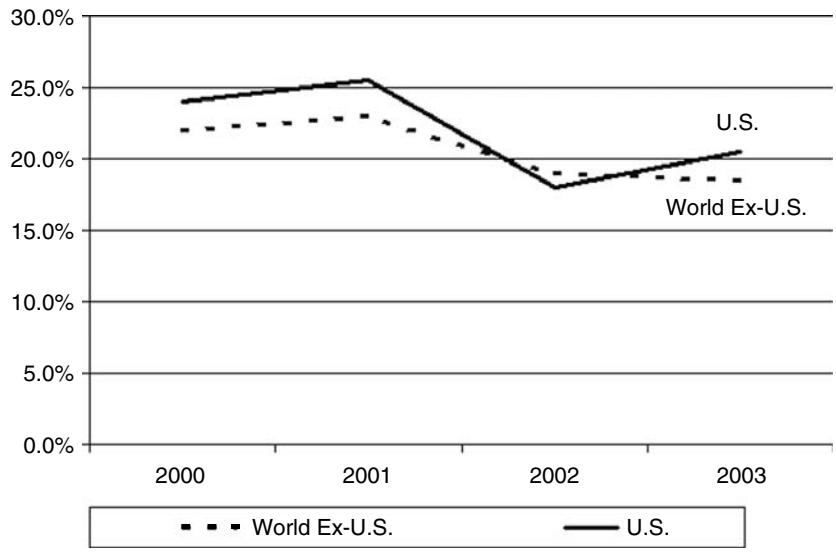
There has been much open debate and criticism claiming that the increased cost of complying with U.S. corporate governance regulations has hurt U.S. competitiveness and driven money away from the U.S. markets. The truth is not nearly this simple.

The price-earnings ratios of U.S. markets have not declined at a greater rate than other markets, suggesting the United States has not lost its competitiveness. Another concern is that foreign filers would flee the U.S. exchanges due

2006 Word Bank Governance Elements	Percentile Ranking (0–100)					
	Average	Canada	Australia	Germany	UK	US
Voice and Accountability	**92.0**	94.2	93.8	95.7	92.8	83.7
Political Stability	**70.2**	80.3	76.9	75.0	61.1	57.7
Government Effectiveness	**94.2**	97.2	95.7	90.5	94.8	92.9
Regulatory Quality	**94.6**	94.1	96.1	91.2	98.0	93.7
Rule of Law	**94.1**	96.2	94.8	94.3	93.3	91.9
Control of Corruption	**93.1**	94.2	95.1	93.2	93.7	89.3

Source: Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, ''Governance Matters V: Governance Indicators for 1996–2005'' (World Bank, July 2006).

EXHIBIT 66.3 2005 WORLD BANK GOVERNANCE RANKINGS: SIX ELEMENTS OF GOVERNANCE FOR THE TOP RANKED COUNTRIES



Sources: Standard & Poor's and *Wall Street Journal*, January 25, 2007.

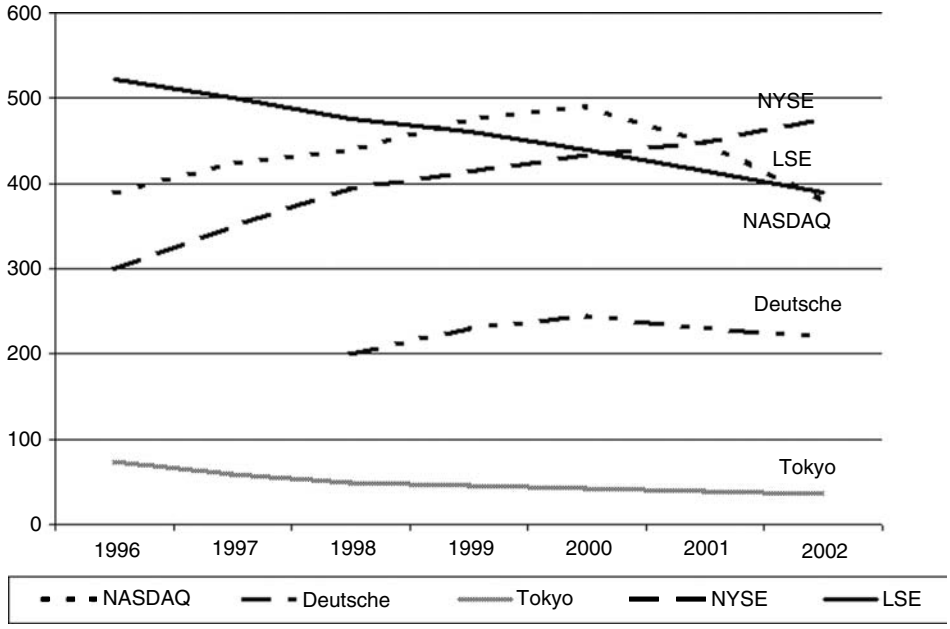
EXHIBIT 66.4 P/E RATIOS U.S. STOCKS VERSUS WORLD STOCK AVERAGE

to increased regulations. While NASDAQ foreign listings have declined, NYSE foreign listings have actually increased in the United States. For the same period the London (LSE), Tokyo, and Deusche have all declined or remained flat.

There has also been a major concern that increased regulations have driven equity capital to the private equity firms as measured as a percent of total mergers and acquisitions. While there has been a significant growth in equity buyouts, the U.S. rate is lower than the European rate.

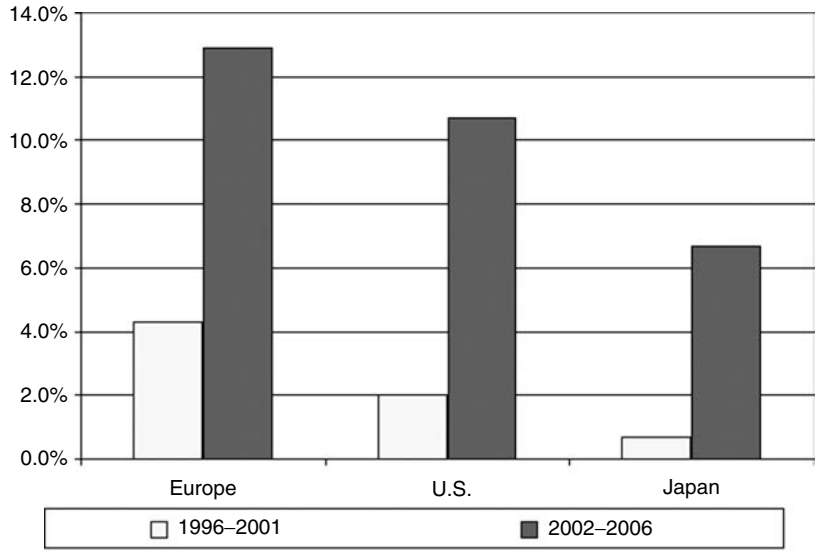
The United States has lost significant ground in attracting initial public offerings (IPOs). During the 1990s, it enjoyed about 40 to 45 percent of the global IPO market. The rate is now about 20 percent. Exhibits 66.4 through 66.7 illustrate these points.

Beyond the hard statistics, the United States has seen a major loss of prestige in the IPO markets. In 2006, only one of the top 20 global IPOs was listed in the United States. Five years ago, over 40 percent of major IPOs were listed in the United States. This concern sparked the creation of a private sector group that has the backing of U.S. Treasury Secretary Henry Paulson. The group, called the Committee on Capital Markets Regulation, has created a variety of suggestions to reduce regulatory burdens, substantially lower litigation levels, and improve U.S.-based IPOs. Litigation cost the United States $3.5 billion in 2006. As a comparison, litigation costs in 1995 were only $150 million. The United States still leads the world's financial markets with a 46 percent share,



Source: World Federation of Exchanges and *Wall Street Journal*, January 25, 2007.

EXHIBIT 66.5 FOREIGN LISTINGS ON MAJOR EXCHANGES



Source: Thomson Financial and *Wall Street Journal*, January 25, 2007.

EXHIBIT 66.6 PRIVATE EQUITY BUYOUTS AS A SHARE OF TOTAL M&AS

Source: Thomson Financial and *Wall Street Journal*, January 25, 2007.

EXHIBIT 66.7 SHARE OF GLOBAL IPO PROCEEDS BY STOCK EXCHANGE

compared to 11 percent for Japan, 9 percent for the UK, and 1 percent for Hong Kong. The premium that foreign filers enjoy for U.S.-based listings is declining, especially in countries with improving corporate governance. The premium is still sizable at about 30 percent, but down from the 50 percent levels enjoyed in the late 1990s. The United States is still the most popular destination for foreign capital, attracting over $2.2 trillion in 2005. This is an increase of over 75 percent in three years.[7]

66.5 HIGHER U.S. UNDERWRITING FEES DRIVE UP IPO COSTS

The City of London Corporation commissioned Oxera Consulting to compare the relative IPO costs across the major exchanges. In comparing U.S. and UK IPO costs, Oxera found that the higher underwriting fees charged in the United States were the main cause for higher U.S. costs. Oxera found London too competitive with Euronext and the Deutsche Boerse. These findings are very significant in that the UK, like the United States, has very high regulatory standards and the United States has embraced the UK's Combined Code as a best practice in corporate governance. The study found no evidence of significant differences in

legal, accounting, and advisory fees across the major exchanges, but higher U.S. legal and auditing costs were attributed to the Sarbanes-Oxley Act (SOX).[8]

The most compelling message in the Oxera report is that the increased costs of U.S. corporate governance have not given it an advantage over the UK. To the contrary, higher U.S. compliance costs hurt U.S. competitiveness against the London markets. The study noted that individual company costs can vary widely from the averages, depending on home country, size, and industry. The larger the size, the better the clustering of analysts within an industry, and the closer the integration from the country of origin and the place of raising capital all lead to lower costs.[9]

66.6 IMPROVED GOVERNANCE DOES NOT TRANSLATE INTO HIGHER GROWTH RATES

It would be nice to report that improved governance will be rewarded in the United States and other nations by improved gross domestic product (GDP) growth rates. Unfortunately, the reverse appears to be the case. For the United States and the other top five GDP nations, as measured by purchasing power parity (PPP), there appears to be a strong negative correlation between GPD growth and World Bank governance ratings. China and India enjoy among the highest growth rates but score poorly in governance ratings. Conversely, the United States, Germany, and Japan enjoy high rates of governance, but relatively low rates of growth when compared to the 200 nations ranked by the CIA Factbook. (See Exhibit 66.8.)

66.7 INVESTOR SURVEYS INDICATE DISSATISFACTION WITH U.S. CORPORATE GOVERNANCE

The *Wall Street Journal Online* and Harris Interactive published a poll in October 2006 showing that about half of American investors look to corporate boards to oversee governance, yet many of them lack confidence in boards' ability to do so. The same poll found that less than one quarter of investors look to CEOs

Top 5 GDP (PPP) Nations	GDP growth Rate (CIA Fact Book, Jan. 2007)				WB 2006 Governance Six Elements		Standard Deviation
	Grade		%	Global Rank	Grade		
China	**A+**	4.3	10.5%	10	**D**	1.0	**2.3**
Germany	**F**	0.0	2.2%	184	**A**	4.0	**2.8**
India	**A**	4.0	8.5%	21	**C**	2.0	**1.4**
Japan	**D**	1.0	2.8%	169	**A–**	3.5	**1.8**
US	**D**	1.0	3.4%	146	**A**	4.0	**2.1**

EXHIBIT 66.8 GDP GROWTH RATES VERSUS WORLD BANK GOVERNANCE RATINGS

to oversee governance and hold the position of chairman of the board, while 39 percent of believe an independent director should hold the job of chairperson.[10]

Investors typically indicate disappointment in the Sarbanes-Oxley Act. Only one-quarter feel the act has improved the control of corporate compensation, an issue of such concern that President Bush called for corporate America to rein in excessive C-level paychecks during a February 2007 press conference. In spite of the ongoing publicity and corporate complaints about its costs, only one-third of investors feel SOX has improved financial transparency, while only half expressed trust in the accuracy of financial reporting.[11] The loss of investor confidence following a series of highly publicized scandals was the main driver for the legislation, and these poll results must be a major disappointment to regulators.

Asked about their ability to trust that companies "provide complete and accurate financial information upon which they can make investment decisions," about half of investors said they can trust companies, compared with 42 percent who said they disagree.

66.8 EXECUTIVE COMPENSATION

Executive compensation has become a major issue in the United States because of what is viewed as a wide disparity between employee and executive compensation. The issue is getting more attention in the past few years, but is not new. Shareholder and board unhappiness with excessive executive compensation led to a variety of proposed reforms in the past 20 years—the most popular of which was stock options. Unfortunately, stock options have presented their set of issues as well—discussed in detail in the stock option issues chapter.

U.S. executives of very large organizations are paid much more than their Japanese or EU counterparts. The disparity drops for smaller companies, and stock and stock options make up most of the difference. On average, the CEOs of companies with sales over $30 billion receive compensation that is higher than the average employee of other countries by the following multiples:

- Japan—17 times higher
- Germany and France—30 times higher
- United States—400 times higher[12]

One of the reasons offered for the large disparity include the greater wiliness and ability of U.S. executives to move around looking for the best compensation deals. Another reason offered is that there is a greater tolerance for inequality in the United States.

The large disparity has sparked shareholder actions, including a movement for a nonbinding advisory vote on executive compensation in at least 60 companies. The SEC's new rules will provide greater transparency into executive compensation. Under the existing rules, executives could hide compensation as

perks, deferred compensation, valuing stock options, pensions, changes in control agreements, and dividends on restricted stock.[13]

The new Democratic-controlled Congress is likely to push for greater shareholder involvement in executive compensation. Such actions would follow the British model. In 2003, the UK passed legislation giving shareholders a voice in compensation. While UK executives have historically made less than their U.S. counterparts, their pay has increased at rates higher than in the U.S. The increased dialogue between shareholders and management has pushed more compensation in bonuses and away from large salary increases. Large UK investors are using the British model to push the U.S. SEC to adopt similar regulations.[14]

66.9 SUGGESTIONS TO IMPROVE BOARD OF DIRECTOR GOVERNANCE

Martin Lipton, a founding partner of Wachtell, Lipton, Rosen & Katz, specializes in advising major corporations on mergers and acquisitions and matters affecting corporate policy and strategy and has written and lectured extensively on these subjects. He served as Special Counsel to the City of New York in connection with the fiscal crisis (1975–1978); Special Counsel, United States Department of Energy (1979–1980); and Acting General Counsel, United States Synthetic Fuels Corporation (1980). Lipton also served as counsel to the New York Stock Exchange Committee on Market Structure, Governance, and Ownership (1999–2000), as counsel to, and member of, its Committee on Corporate Accountability and Listing Standards [Corporate Governance] (2002) and as chairman of its Legal Advisory Committee (2002–2004). Mr. Lipton provides a good checklist of areas boards should address to improve oversight and stewardship.[15]

The Role and Duties of the Board. "The past 20 years have witnessed a transition from the advisory board to the monitoring board. While the board has always had a dual role as a resource and advisor for management, on the one hand, and as an independent agent of shareholders on the other, in recent years government regulators and activist shareholders, empowered by the reaction to the Enron-type scandals and often in competition with each other, have been tipping this balance with increasing force in favor of monitoring. But it is still generally acknowledged that a combination of the two is necessary, and that only a collegial board can function effectively over the long run. To be truly effective, each board must find the right balance between monitoring and advising as to strategy. Finding this balance is the critical starting point in any consideration of how to structure the membership and the operations of a board."

Tone at the Top. "One of the most important factors in ensuring that a board functions effectively and meets all of its responsibilities is having the right tone at the top of the corporation. The tone at the top will form the culture of the corporation and permeate the corporation's relationship not only with investors, but also with employees, customers, suppliers, local communities, and

other constituents. If the CEO and senior management are not personally committed to high ethical standards, principles of fair dealing, full compliance with legal requirements, and resistance to Wall Street pressures for short-term results, no amount of board process or corporate compliance programs will protect the board from embarrassment. The board should participate in creating the corporate culture and should periodically review with the CEO what the CEO and senior management are doing to set the right example and how it is being communicated to all employees and constituents of the corporation."

Transparency. "The board's vision for the corporation, including its commitment to ethics and zero tolerance for compliance failures, should be set out in the annual report and communicated effectively within the corporation."

CEO Selection and Succession Planning. "In addition to setting the tone at the top, the other most important job of the board is selecting and evaluating the CEO and the senior executive leadership of the corporation and planning for their succession. As the central interface between the corporation and what stands outside it—for example, society, the economy, technology, markets, customers, and the media—the CEO plays the key role in the corporation. There are no prescribed procedures for planning succession and selecting the CEO, and a board should fashion the principles and procedures it deems appropriate. In fulfilling its CEO selection and succession function, the board should recognize that by itself competence is not enough. The integrity and dedication of the CEO is critical in enabling a board to meet all of its responsibilities. In large measure, the fates of the board and the CEO are each in the hands of the other."

Effectiveness of the Board. "It has been suggested that a board's failure to allot adequate time to carry out its duties could call into question whether it had acted in good faith. In addition to scheduling regular board and committee meetings to provide ample time for the regular business of the board, boards should consider the desirability of an annual two-to-three-day board retreat with the senior executives at which there is a full review of the corporation's financial statements and disclosure policies, strategy and long-range plans, budget, the company's mission, succession planning, and current developments in corporate governance. Retreats might be rotated among locations close to one of the corporation's operations, so as to give the directors an opportunity to become acquainted with a number of the corporation's operations. During the retreat, meals and social activities may be arranged in a manner that encourages the directors to get to know the senior executives on a one-on-one basis. Corporations should also provide comprehensive orientation for new directors so as to acquaint them with the corporation's strategy, long-range plans, financial statements, properties and operations, corporate governance guidelines, and senior executives. The annual retreat could satisfy a major portion of such an orientation. In addition to orientation, corporations should provide education programs for continuing directors, both to enhance their skills as directors as well as to help them stay abreast of regulatory and corporate governance developments."

Separating Roles of Chairman and CEO; Lead Director. "Most American companies have traditionally had a single individual who combines the roles of both chairman of the board and CEO. While some shareholder activists have called for the separation of these roles, most institutional shareholders and their advisors leave this matter to the discretion of the board, provided that there is an independent director who presides over executive sessions of the board. While there is no formal requirement in the NYSE rules or in the Sarbanes-Oxley Act that a company have a lead director, the independent directors should have a leader who is not also the CEO. Whether he or she is called the lead director, the nonexecutive chair, or the presiding director, this leader should have four key roles:

1. Be available to discuss with the other directors any concerns they may have about the company and its performance and relay these concerns, where appropriate, to the full board.
2. Be available to consult with the CEO regarding the concerns of the directors.
3. Be available to be consulted by any of the senior executives of the company as to any concerns the executive might have.
4. Preside at executive sessions of the board. In order to be effective, the lead director should be a senior person who is highly respected and regarded by the CEO and the other directors.

The lead director is not an officer and would not have any of the formal duties of a chairman of the board, but he or she is the director who would assume leadership of the board if a need to do so should arise. A company might either have a single individual designated as a lead director or have a presiding directorship through which the committee chairs rotate. If a lead director is designated, the NYSE requires his or her name to be disclosed in the annual proxy statement. Alternatively, a company may disclose the procedure by which a presiding director is selected for each executive session."

Independence. "Today, there is an overemphasis on board independence that risks losing sight of the importance of promoting the sort of board dynamic that can most effectively lead to a well-functioning board and an effective partnership between the board and senior management. Although the NYSE requires only that a majority of the board be independent, today most boards have only one or two directors who are not independent: the CEO and maybe one other current or former officer. Nevertheless, many of the shareholder advisory services, institutional investors, and academic gadflies are continuing to urge (in some cases, demand) that all directors other than the CEO be independent and that social and philanthropic ties among and between the directors and the CEO be considered as impugning, if not destroying, independence. These types of requirements and restrictions are the antithesis of the kind of collegiality and relationship with the CEO that is necessary for the board and CEO together to promote the appropriate tone at the top, to agree on the corporate mission and to work collectively to

enhance the corporation's business. What companies need are directors who possess sufficient character and integrity to allow them to make judgments unaffected by considerations affecting themselves or those with whom they have relations. The concept of directors as remote strangers and the board as the agency for the discipline of management, rather than as advisor to management in setting the strategic course of the corporation, is contrary to all prior experience and will not lead to better performance. The tension between the new norms of independence and the overarching objective of better performance, unless modulated and maintained in perspective, can cause the former to overwhelm the latter. That said, as a general rule, a director must be careful in the current environment to make full and complete disclosure of any relationships or transactions that could be deemed to affect independence. Many relationships that may have been considered commonplace in the past (such as a director's involvement with a nonprofit organization that is supported by the company) may, in today's skeptical environment, cast doubt on the level of that director's independence when viewed with hindsight after a crisis has arisen. This is not to say that all such relationships should be prohibited, but rather that all should be considered in assessing a director's independence. A practical way to deal with those situations is that where such relationships might raise an issue as to the independence of the directors acting on a particular matter, consideration should be given to delegating that matter to a committee of directors, each of whom is free of such relationships."

Corporate Strategy. "Approval of the corporation's long-term strategy is a key board function. Strategy should be formulated initially by management and then developed fully in an interactive dialogue with the board. Many companies find it productive to include an annual strategy review in a board retreat as described earlier."

Nomination of Director Candidates. "Under the existing corporate governance system, a company's nominating committee nominates candidates for membership on the company's board. Shareholders can propose potential director candidates to the company's nominating committee, which under the NYSE rules must be composed entirely of independent directors. The nominating committee has a duty to consider bona fide candidates and to nominate directors that it believes will best serve the interests of the company and its shareholders. In evaluating potential director candidates, whether they are proposed by management or by shareholders, the nominating committee should use the same fundamental criteria. The foremost criterion is competence: Boards should consist of well-qualified men and women with appropriate business and industry experience. The second important consideration is collegiality. A balkanized board is a dysfunctional board; a company's board works best when it works as a unified whole, without camps or factions and without internal divisions. The nominating committee should also try to ensure that the board consists of individuals who understand and are willing to shoulder the time commitment necessary for the board to effectively fulfill its responsibility to advise and monitor management.

To this end, companies should consider including in their corporate governance guidelines policies limiting the number of boards on which a director may sit. Those guidelines should also address director tenure. Companies should consider whether it would be advisable for them to impose term and age limits on directors. There is no formula for the perfect board. Strong, independent directors are essential to proper board functioning, but so too are elusive qualities such as collegiality, sense of common purpose, energy, industry knowledge, business sense, and trust. The nominating committee should have the flexibility to determine the mix of qualifications and attributes that is best suited to the specific needs of the corporation."

Confidentiality and the Role of Directors Outside the Boardroom. "A board should function as a collegial body, and directors should respect the confidentiality of all discussions that take place in the boardroom. Confidentiality is essential for an effective board process and for the protection of the corporation and its stockholders. Moreover, directors generally owe a broad legal duty of confidentiality to the corporation with respect to information they learn about the corporation in the course of their duties. Maintaining confidentiality is also essential for the protection of the individual directors, since directors can be responsible for any misleading statements that are attributable to them. Even when a director believes the subject matter of his or her statements is within the public domain, it is good practice for individual directors to avoid commenting on matters concerning the corporation. A director who receives an inquiry with respect to the corporation from outside the corporation may or may not have all of the relevant information and his or her response could involve the corporation, as well as the director, in a disclosure violation. Directors also should respect the role of the CEO as the chief spokesperson for the corporation. They should generally not engage in discussions with outsiders concerning corporate business unless specifically requested to do so by the CEO or the board. Where it is necessary for outside directors to speak on behalf of themselves or the corporation, here too it is best for one member of the board to be designated as the board's spokesperson. Where a board has a nonexecutive chairman or a lead director, under certain circumstances it may also be appropriate for the chairman or lead director to speak on behalf of the corporation, particularly within the ambit of those directors' special roles. In the ordinary course, all such matters should be handled in close consultation with the CEO so as to avoid confusion in the corporation's public statements and posture."

Committees of the Board. "The NYSE requires a listed company to have an audit committee, a compensation committee, and a nominating-governance committee, each comprised solely of independent directors. The requirement that a committee be composed of only independent directors does not mean that the CEO (and other employees) should be excluded from all the discussions or work of the committee. Indeed, it would be virtually impossible for the committees to function effectively without the participation of the CEO. All compensation

matters, including the CEO's compensation, should be discussed with the CEO, and all governance and director nomination matters should be discussed with the CEO. While the final determination is that of the committee, there is no restriction on full discussion with the CEO. The committees have the authority to retain consultants, but there is no requirement that the compensation committee retain a compensation consultant or that the nominating-governance committee retain a search firm, if the committee believes that it does not need such assistance."

"All companies, as part of their broader governance reviews, should carefully consider which directors satisfy the requirements for service on committees. Questionnaires may be used to determine and document both independence and qualification for committee assignments. In addition to these core committees, boards may wish to establish additional standing committees to meet their ongoing governance needs, such as a risk management committee (if this function is not being performed by the audit committee), a compliance committee, or a committee on social responsibility. Boards may also use special committees from time to time either to deal with conflict transactions (such as a management buyout) or other major corporate events (such as shareholder litigation or a hostile takeover bid) or to address particular special investigations or projects. While the use of special committees is appropriate and useful in many circumstances, such committees are also often used in situations where it might be best to keep the matter in question before the full board (or before all of the outside members of the full board). Special committees can sometimes become divisive in sensitive situations, and there is a risk that the special committee and its outside advisors may take a matter in a direction that would be different than that desired by the full board. Especially in matters of great sensitivity, it is often preferable for all directors (or at least all outside directors) to remain active in dealing with the matter."

"The work of the board will be facilitated by establishing the appropriate relationship between the board as a whole and each of its committees, so that the work of the committees is neither duplicated nor ignored by the board. The significant actions of the committees should be understood by the board as a whole and integrated into the overall work of the board. In order to enable both the board and its committees to deal with any special problems that may arise in the course of performing their duties, the board and its standing and special committees should have the authority to engage independent advisors where appropriate. That said, this authority should be used sparingly; as a general rule, a board or board committee should resort to it only when there is a real conflict or some other genuine need for independent or specialized advice. More often than not, a corporation's own general counsel or CFO can provide more pertinent advice and insight than that available from outside sources; so too can outside counsel that has a substantial continuing relationship with the corporation, rather than 'independent' counsel that has had no relationship with the corporation."

The Audit Committee. "The post-Enron reforms have invested the audit committee with a special role in corporate governance. In large measure, the audit

committee has become the principal means by which the board monitors financial and disclosure compliance. Accordingly, boards should carefully select audit committee members and, to the greatest extent possible, be attuned to the quality of the audit committee's performance. In view of the audit committee's centrality to the board's duties of financial review, it is also important for the board as a whole to receive periodic reports from the audit committee and to be comfortable that the audit committee, the auditors and management are satisfied that the financial position and results of operations of the corporation are fairly presented."

Board and Committee Agendas. "The board and its committees should be proactive in working with senior management and the general counsel in setting their agendas for the year as well as for each board or committee meeting. While it is management, not the board, that must initiate the strategic and business agenda for the company, including regulatory and compliance goals, directors should take a leadership role in defining the bounds of their oversight and responsibilities. The meeting agendas and the overall annual agenda should reflect an appropriate division of labor and should be distributed to the board or committee members in advance."

Executive Sessions. "The NYSE requires the nonmanagement directors to meet in regularly scheduled executive sessions of the board in which management is not present. Each board should determine the frequency and agenda for these meetings. They provide the opportunity for meaningful review of management performance and succession planning. In addition, they are a safety valve to deal with problems. They should not be used as a forum for revisiting matters already considered by the full board. The executive sessions should not usurp functions that are properly the province of the full board."

Charters, Codes, Guidelines, and Checklists. "The audit, compensation, and nominating-governance committees are required to have charters. The corporation is required to have a code of ethics. The board is required to have corporate governance guidelines and, as noted, there is no end to the number of recommended checklists designed to assist corporations in complying with Sarbanes-Oxley, SEC regulations, and NYSE rules. All of these are to some extent useful in assisting the board and committees in performing their functions and in monitoring compliance. However, there is a tendency to expand the scope of charters and checklists to the point that they are counterproductive. If a charter or checklist requires review or other action and the board or committee has not taken that action, the failure may be considered evidence of lack of due care. The creation of charters and checklists is an art that requires experience and careful thought. It is a mistake to copy the published models. Each corporation should tailor its own charters and checklists, limiting them to what is truly necessary and what is feasible to accomplish in actual practice. In order to be state of the art, it is not necessary that the corporation have everything someone else has. Charters and checklists should be carefully reviewed each year to prune unnecessary items and to add only those items that will in fact help directors in discharging their duties."

Meeting Minutes. "Careful and complete minutes should be kept of all board and committee meetings. The minutes should reflect the discussions and the time that was spent on significant issues, both in the meeting and prior to the meeting. The minutes should also reflect all those who were present at the meeting and the matters for which they were present or recused. Increasingly, courts and regulators have raised questions about the amount and scope of attention that was spent on a matter when the minutes did not contain an adequate description. Depending on the matters considered at executive sessions, it may be appropriate to have summary minutes or in some cases very extensive or even verbatim minutes of such sessions."

Executive Compensation. "This is today's most high-profile corporate issue and a major focus of shareholder activism. Virtually everyone who has weighed in on this issue agrees that executive compensation should be aligned with long-term corporate performance and shareholder value. In addition, most companies, including well-performing ones, need to engage in recruiting and retention efforts to attract, and prevent the loss of, qualified individuals. There is a wide spectrum of views as to how to achieve the agreed objectives. The only really useful advice is thoughtful process, full disclosure and recognition by the compensation committee that it should not be deterred by media and gadfly attention from doing what it feels is in the best interests of the corporation. Executive compensation should directly link the interests of senior management and the long-term interests of shareholders. Some organizations, such as the Business Roundtable, have recommended the use of performance thresholds to achieve this. In order to ensure that compensation and severance packages are justifiable, members of the compensation committee should fully understand all the costs and benefits of the compensation arrangements that they are considering. Particular attention should be paid to severance arrangements and to all benefits provided to senior management in connection with termination of employment. Perquisites should be kept reasonable and a line should be drawn between business and personal expenses. Both the Business Roundtable and the Blue Ribbon Commission on Executive Compensation of the National Association of Corporate Directors emphasize the importance of transparency and full disclosure of compensation packages. The minutes of the compensation committee should reflect discussion and full understanding of every element of the compensation approved."

Board, Committee, and CEO Evaluations. "The NYSE requires annual evaluations. Many consulting firms have published their recommended forms and procedures for conducting these evaluations. Consultants have also established an advisory service in which they meet with the board and committee members to lead them through the evaluation process. Each board needs to decide how to conduct its evaluation. In making the decision, it should be noted that it is not required that the board receive outside assistance and it is not required that multiple-choice questionnaires and/or essays be the means of evaluation. If a board prefers to do the evaluation by discussion at meetings, that is acceptable. It

should also be noted that documents and minutes created as part of the evaluation process are not privileged and care should be taken to avoid creating ambiguous records that may be used in litigation against the corporation and the board."

Shareholder Activism; Proxy Advisors; Majority Voting in Director Elections. "One of the most visible by-products of the Enron-type scandals is the increase in shareholder-sponsored precatory proxy resolutions and the high level of shareholder support that they are able to command. On some issues, mostly related to antitakeover defenses, shareholder proposals now routinely receive majority support. One of the explanations for such shareholder support is the demise of case-by-case voting by institutional shareholders. Today, institutional shareholders typically subscribe to the services of proxy voting advisors, such as Institutional Shareholder Services (ISS), to provide analysis or advice with respect to shareholder votes. These proxy voting advisors publish proxy voting guides setting forth blanket voting policies on a variety of common issues that are frequent subjects of shareholder proposals. Institutional shareholders typically do not review individual shareholder proposals on a company-by-company basis. Instead, they rely heavily on these proxy voting guidelines, regardless of an individual company's performance or governance fundamentals. As a result, many shareholder votes are foreordained by a voting policy that is applied to all companies without reference to the particulars of a given company's situation.

"In dealing with shareholder proposals, the board should regularly review the corporation's shareholder relations programs and consider whether it is appropriate for the board to have greater interaction with shareholders. Where the corporation has performance or compliance issues, direct contact between shareholders and nonmanagement directors may forestall a proxy initiative by shareholders. In addition, the corporation should weigh carefully opposition to shareholder proxy resolutions that can be accommodated without significant difficulty. Today, it is prudent to do a risk-reward analysis of shareholder resolutions, rather than to routinely oppose them. As companies spend more time and effort to consider shareholder proposals, it might make sense to formalize the process by which this is done. By paying serious attention to shareholder proposals, and by being proactive in shareholder communications and disclosure, boards are most likely to create the right environment for acting on shareholder resolutions even when the ultimate determination may be to reject them.

"Currently the effort by activist shareholders to persuade corporations to adopt majority voting for election of directors has developed significant shareholder support. The Council of Institutional Investors has written to 1,500 corporations requesting that they adopt majority voting, the Committee on Corporate Laws of the American Bar Association has released a discussion paper highlighting the issues involved in switching to majority voting and a committee in Delaware is considering whether its corporation law should be amended. General Electric, Pfizer, Office Depot, and Disney, among others, have amended their corporate governance guidelines to require that any director who receives a majority

of 'withhold' votes submit his or her resignation to the board, leaving the outcome in the hands of the board.

"In November 2005, ISS announced a majority voting policy providing that ISS will consider not recommending a vote for a precatory or binding shareholder proposal requiring that directors be elected by an affirmative majority of votes cast if the company has adopted a formal majority-vote-corporate-governance principle that presents a 'meaningful alternative.' The governance principle must incorporate the following elements to adequately address each new and incumbent director nominee who fails to receive an affirmative majority of votes cast in an election:

- Annual proxy statement disclosure of the established guidelines for the process to be followed regarding the nominee;
- A clear and reasonable timetable for all decision-making regarding the nominee;
- Management of the process by independent directors, and exclusion from the process of the nominee at issue;
- An outline of a range of remedies that can be considered regarding the nominee; and
- Prompt disclosure of the final decision in an SEC filing, including a full explanation of how the decision was reached.

"A company adopting such a governance principle should also explain why the principle is the best structure at such time in terms of accountability to shareholders. ISS, in reaching its recommendation on a majority vote proposal, will review a company's history of accountability to shareholders, including taking into account a classified board structure and a history of ignoring majority approved shareholder proposals.

"It is clear today that majority voting will become universal. In light of ISS' position and in an effort to avoid shareholder proposals for proxy inclusion and subsequent requests for no-action relief from the SEC, it is advisable for companies to adopt proactively a corporate governance principle that satisfies the ISS guidelines. Some majority voting proponents are insisting on a true majority vote requirement, rejecting the corporate governance principle approach of a tendered resignation and calling for the majority vote requirement to be included in a company's charter or bylaws and not the corporate governance guidelines. It remains to be seen whether the SEC will permit a company to omit from its proxy statement a precatory or binding shareholder proposal submitted under Rule 14a 8 if the company has addressed the issue in its corporate governance guidelines using a governance principle meeting ISS standards. It also remains to be seen whether a majority voting shareholder proposal which ISS does not recommend favorably (and which the SEC does not permit to be omitted from the proxy statement) will nonetheless garner support of institutional investors and be adopted by shareholders.

"It is important to note that the ISS guidelines require that the corporate governance principle address the situation where the director nominee receives 'withhold' votes from the majority of votes cast, as opposed to a majority of the shares outstanding, notwithstanding my best efforts to convince ISS to adopt the majority of the shares outstanding standard. While I continue to believe that the majority of the outstanding shares standard is the better approach, I recognize that the position is not shared by ISS and some institutional shareholders and, because of the importance of discouraging an adversarial proxy proposal process, I recommend the adoption of a governance principle which satisfies ISS guidelines.

"Given the 'majority of the shares outstanding' approach, one can expect some in the institutional investor community to continue to pressure the NYSE to alter its rules on broker voting for their customers who fail to do so. Wall Street firms have traditionally used their discretionary voting power under NYSE rules to vote in favor of management those shares held in street name for which they have not received voting instructions from their clients. While the NYSE rules do not allow discretionary broker voting in contested situations, the NYSE has taken the position that withhold the vote campaigns are not considered contested situations. It is more important than ever that the NYSE not back away from this position, as doing so would in effect cause the passivity of a satisfied retail shareholder base to shrink the quorum, thereby overemphasizing the withhold vote count.

"Shareholder activism would be further aided by a proposed SEC rule to permit Internet distribution of proxy statements. The proposal would make it less expensive for activist shareholders who are dissatisfied with incumbent directors to wage withhold-the-vote campaigns, or full proxy contests for board representation."

Balancing Short-Term Performance and Long-Term Success. "Activist shareholders, led by hedge funds, which today have aggregate assets of more than $1 trillion, and armed with the threat of withhold-the-vote campaigns against directors, will exacerbate the tension between short-term performance and long-term success of the corporation. This is currently being manifested in the expanding demands by hedge funds to do a massive stock buyback funded by a sale of assets or to sell the entire company. While different in form, this hedge fund pressure raises management and board issues similar to those created by the pressure to give quarterly earnings guidance and then meet the targets."

The Disney Case. "The decision of the Delaware Chancery Court in the Disney case reaffirmed that the business judgment rule is alive and well. The Disney decision also delineated the scope of protection of directors against personal liability for claimed breach of fiduciary duty. Negligence—that is, a failure to use due care—will not result in personal liability unless the director failed to act in good faith. The court ruled that "intentional dereliction of duty, a conscious disregard for one's responsibilities" is an appropriate test for determining whether

a director has acted in good faith. The court ruled that a director fails to act in good faith when the director (1) 'intentionally acts with a purpose other than that of advancing the best interests of the corporation,' (2) 'acts with intent to violate applicable positive law,' or (3) 'intentionally fails to act in the face of a known duty to act, demonstrating a conscious disregard for his duties.' The court also said that although it strongly encourages directors to employ best practices of corporate governance, as those practices are understood at the time a board acts, directors will not be held liable for failure to comply with 'the aspirational ideal of best practices.' In other words, directors will have the benefit of the business judgment rule if they act on an informed basis, in good faith, and not in their personal self-interest, and in so doing they will be free from 'post hoc penalties from a reviewing court using perfect hindsight.'

"There are two principal sources of potential personal liability for directors: state law fiduciary duties and federal securities laws. As affirmed in the Disney case, the business judgment rule protects directors from state law liabilities. If a director acts with due care, does not have a conflict of interest, and believes that he or she is acting in the best interests of the corporation, the director will be protected by the business judgment rule. The guidelines in this memorandum provide directors with a roadmap for staying well within the protection of the business judgment rule.

"The federal securities laws pose a greater threat of personal liability than state law fiduciary duties. The 2004 WorldCom and Enron settlements, in which the directors agreed to personal payments, were federal securities law cases. Directors are liable for material misstatements or omissions from registration statements the company has used to sell securities unless the directors prove that they exercised due diligence. To meet their due diligence requirements, directors must carefully review and understand the registration statements and other disclosure documents that the corporation files with the SEC. In doing so the directors can rely on the accountants with respect to the audited financial statements and on other experts, provided that the directors have no reason to believe that the expert is not qualified or is conflicted or that the disclosure is actually false or misleading. Directors should not merely accept management's representations that a registration statement is accurate, and are well advised to have their corporation's legal counsel present for the directors' review of all SEC disclosure documents and receive the advice of counsel that the process they have followed fulfills their due diligence."

Reliance on Advisers. "The basic responsibility of directors is to exercise their business judgment to act in a manner they reasonably believe to be in the best interests of the corporation and its shareholders. In discharging these obligations, directors are entitled to rely on management and the advice of the corporation's outside advisors. The board should make sure that the corporation's legal counsel, both internal and external, and auditors, both internal and external, have direct access to the board, if ever needed."

Director Compensation. "Director compensation is one of the more difficult issues on the corporate governance agenda. On the one hand, more is being expected of directors today in terms of time commitment, responsibility, and exposure to public scrutiny and potential liability. On the other hand, the higher the director's pay, the greater the chance it will raise an issue of independence. The compensation committee should determine the form and amount of director compensation with appropriate benchmarking against peer companies. It is legal and appropriate for basic directors' fees to be supplemented by additional amounts to chairs of committees and to members of committees that meet more frequently or for longer periods of time. The Council of Institutional Investors and other shareholder advisory organizations have recognized the need for adequate director compensation and have published guidelines.

"While there has been a current trend, encouraged by institutional shareholders, to establish stock-based compensation programs for directors, the form of such programs should be carefully considered to ensure that they do not create the wrong types of incentives for directors. In the current environment, restricted stock grants, for example, may be preferable to option grants, since stock grants will align director and shareholder interests more directly and avoid the perception that option grants may encourage directors to support more aggressive risk taking on the part of management to maximize option values. Perquisite programs and company charitable donations to organizations with which a director is affiliated should also be carefully scrutinized to make sure that they do not jeopardize a director's independence or create any potential appearance of impropriety. Where appropriate, such perquisites should be fully disclosed."

Monitoring Performance. "While the corporation laws literally say that the business of the corporation is to be managed by or under the direction of the board of directors, it is clear that the board's function is not to actually manage, but to oversee the management of the corporation by monitoring the performance of the CEO and senior officers. For the board to monitor performance, the board and management together need to determine the information the board should receive. Here, less can be more. The board should not be overloaded with information. It is not necessary that the board receive all the information that the CEO and senior management receive. The board should receive the information that it determines to be useful to it. The board should consider annually whether it is receiving the appropriate information and make adjustments as necessary. Basically, the board should receive financial information that enables it to readily understand results of operations, variations from budget and trends in the business and the corporation's performance relative to peers. In addition, the board should receive copies of significant security analysts' reports, press articles and other media reports on the corporation. If an article or report raises compliance, performance or other issues, the board should request a satisfactory explanation of the issues raised in the publication, including, if appropriate, what is being done to correct the situation. By tracking these reports and articles, the board

will avoid the possibility of being accused of ignoring problems that were known to others and which could have been known by the directors."

Monitoring Compliance. "As with performance, the board should monitor legal and regulatory compliance by the corporation. The board does not have a duty to ferret out compliance problems. It does, however, have a duty to take appropriate action when it is aware of a problem and that management is not properly dealing with it. In normal situations, it is sufficient for the board to review compliance matters and litigation semiannually. This may be done directly by the board or through the audit committee or another committee. However it is done, it is a desirable practice for the board or the committee to meet regularly in executive session with the general counsel of the corporation. Where there is a serious investigation or litigation that is being handled by outside counsel, such counsel should report directly to the board or the committee. In addition, the board should oversee an annual review of the corporation's compliance and governance programs and its information and reporting systems and receive the opinion of the general counsel as to their adequacy.

"In performing its monitoring function, the board should be sensitive to red flags and yellow flags. When such flags are raised, the board should observe and investigate as appropriate and document its monitoring activities in minutes that accurately convey the time and effort directors devote to decision making, even when the outcome is to take no action.

"The federal sentencing guidelines also promote comprehensive compliance procedures and careful monitoring by requiring that directors be knowledgeable about compliance programs, be informed by those with day-to-day responsibility over compliance, and participate in compliance training. The guidelines provide that an effective compliance program monitored by the board may be a mitigating factor in a prosecutor's decision whether or not to charge a company with wrongdoing."

Crisis Management. "Perhaps the most important test of a board comes in times of crisis. Boards need to be proactive in taking the reins in the context of any governance, compliance, or business crisis affecting the corporation. At the same time, boards need to be cautious not to overreact to any given situation and thereby create a crisis. Boards have responded to recent crises with varying degrees of success. It appears that many boards have functioned quite well in taking a careful measure of the situation and putting in place the right procedures for obtaining the necessary information about the issues facing the corporation and developing the right strategies for responding to the situation and rectifying any management, disclosure, or legal/compliance deficiencies. Others, however, appear either to have overreacted or to have placed matters in the hands of lawyers, accountants, and other outside experts and thereby lost control of the situation to those outsiders. And, in some instances the crises themselves appear to have arisen in large part from the failure of management and the board to be proactive in reacting to earlier warning signs.

"The first decision a board must make during a crisis is to decide whether the CEO should lead the corporation through the crisis. If the CEO is part of the problem or is otherwise compromised or conflicted, someone else—often one of the other directors—should take a leadership role. If the CEO is not compromised or conflicted, the CEO should lead the corporation's response to the crisis.

"Each crisis is different, and it is difficult to give general advice that will be relevant to any particular crisis without knowing the facts involved. That said, in most instances when a crisis arises, the directors are best advised to manage through that crisis as a collegial body working in unison. While outside advisers (counsel, auditors, consultants, and bankers) can play a very useful and often critical role in getting at all of the relevant facts of a given situation and in helping to shape the right result, the directors should maintain control and not cede the job of crisis management to the outside advisers. And, while there is often the impulse to resign from the board upon the discovery of a crisis, in most instances, directors are best served by staying on the board until the crisis has been fully vetted and brought under control."

Whistle-Blowers. "Boards, and in particular audit committees, are required to establish procedures to enable employees to confidentially and anonymously submit concerns they might have regarding the company's accounting, internal controls, or auditing matters. In addition, companies are subject to potential civil, and in some cases criminal, liability if they can be shown to have taken retaliatory action against a whistle-blower who is an employee. In responding to these new constraints, there can be a temptation to establish a special committee of independent directors to investigate every single whistle-blower complaint. This temptation should be resisted in favor of a procedure that filters whistle-blower complaints, as such investigations can be extremely disruptive. The SEC has urged companies to appoint a permanent ombudsman or business practices officer to receive and investigate complaints. Boards should ensure the establishment of an anonymous whistle-blower hotline and a well-documented policy for evaluating whistle-blower complaints, but they should also be judicious in deciding which complaints truly warrant further action."

Review of Controls and Risk Management. "The board should also—whether directly or through the audit committee—review whether management has adopted and implemented proper risk assessment and risk management policies and procedures. The risks that a company might face include business risks (such as risks posed by defective products, violation of environmental requirements, accidents, and political changes); financial risks (such as risks posed by financial asset composition, derivative securities, structured financing, contingencies, and guarantees); legal risks; and reputation risks. The board should review whether each category of risk is adequately addressed by the company's risk management procedures.

"It is an important responsibility of management, and a key monitoring role for the board, to establish and maintain an adequate internal control structure and

procedures for financial reporting and compliance with law, including applicable SEC disclosure requirements. The SEC rules implementing Section 404 of the Sarbanes-Oxley Act require management to prepare reports on internal controls and the independent auditor to attest to those reports as part of its audit. The rules also call for a quarterly evaluation and certification by management of a company's internal controls and procedures for financial reporting. Directors should pay careful attention to whether management has invested sufficient resources and energies in the company's control and risk monitoring and management infrastructure. The board (through the audit committee) should satisfy itself (by getting regular reports from the management and the internal auditor) that the company's existing internal control systems provide for the maintenance of financial records in a way that permits preparation of financial statements in accordance with GAAP and gives 'reasonable assurance' of accuracy in financial reports, and that management designs and supervises processes that adequately identify, address and control compliance risks. That said, while reasonable assurance is a high standard, it is not an absolute, and boards should avoid overreaction to the discovery of deficiencies."

Major Transactions. "Board consideration of major transactions, such as acquisitions, mergers, spinoffs, investments and financings, needs to be carefully structured so that the board receives the information necessary in order to make a reasoned decision. This does not mean that outside advisors are necessary, even for a very large transaction. If the corporation has the internal expertise to analyze the requisite data and present it in a manner that enables the board to consider the alternatives and assess the risks and rewards, the board is fully justified in relying on the management presentation without the advice of outside experts. There is no need for the board to create a special committee to deal with a major transaction, even a hostile takeover, and experience shows that a major transaction is best addressed by the full board. Management should build a strong foundation to support a major transaction, including an appropriate due diligence investigation. The board should have ample time to consider a major transaction, including in cases of complicated transactions and agreements a two-step process with the actual approval coming only after an initial presentation and the board having had time for reflection."

Related-Party Transactions. "Generally boards are not comfortable with related-party transactions and today most companies avoid them. However, there is nothing inherently improper about transactions between a corporation and its major shareholders, officers, or directors; such transactions are often in the best interests of a corporation and its shareholders, offering efficiencies and other benefits that might not otherwise be available. It is entirely appropriate for an informed board, on a proper record, to approve such arrangements through its disinterested directors. As a matter of compliance and best practices, however, and particularly in the current environment, the corporation should give careful attention to all

related-party transactions. Full disclosure of all material related-party transactions and full compliance with proxy, periodic reporting, and financial footnote disclosure requirements is essential. Management should make sure that all related-party transactions have been fully and carefully reviewed with the board. The board should reevaluate the corporation's policies and procedures for reviewing such transactions on both an initial and ongoing basis and for determining that all continuing related-party transactions remain in the best interest of the corporation. The board should consider assigning to a committee consisting solely of directors who are both independent and disinterested with respect to the transaction under consideration the job of reviewing any newly proposed related-party transactions. The committee should have the authority to hire such outside financial, legal, and other advisers as it deems appropriate to assist it in its evaluation of such transactions."

Indemnification, Exculpation, and Directors and Officers (D&O) Coverage. "The Disney decision notwithstanding, shareholder litigation against directors continues. All directors should be indemnified by the company to the fullest extent permitted by law, and the company should purchase a reasonable amount of D&O insurance to protect the directors against the risk of personal liability for their services to the company. Bylaws and indemnification agreements should be reviewed on a regular basis to ensure that they provide the fullest coverage available. Having in place governance procedures that are responsive to the recent legislative and regulatory initiatives and that reflect best practices, and having a robust record reflecting strong, good-faith efforts to adhere to those procedures, will be helpful in assuring that a court respects the applicability of exculpatory charter provisions.

"D&O coverage provides a key protection to directors. While such coverage has become more expensive in recent years, it is still available in most instances and remains highly useful, despite some recent decisions construing the terms of D&O policies less favorably to the insured. In this regard, it is important to note that D&O policies are not strictly form documents and can be negotiated. Careful attention should be paid to retentions and exclusions, particularly those that seek to limit coverage based upon a lack of adequate insurance for other business matters, or based on assertions that a company's financial statements were inaccurate when the policy was issued. Directors should also consider the potential impact of a bankruptcy of the company on the availability of insurance, particularly the question of how rights are allocated between the company and the directors and officers who may be claiming entitlement to the same aggregate dollars of coverage. To avoid any ambiguity that might exist as to directors' and officers' rights to coverage and reimbursement of expenses in the case of a bankruptcy, many companies are purchasing separate supplemental insurance policies covering only directors and officers and not the company (so-called side-A coverage) in addition to their normal policies, which cover both the company and the directors and officers individually."

66.10 CONCLUSION

The primary issues and public debate around U.S. corporate governance include the cost of implementing the internal control improvements of the Sarbanes-Oxley Act, the composition and proactiveness of corporate boards, excessive executive compensation, the competitiveness of U.S. markets in attracting global capital, growing minority shareholder demands for a greater role in corporate decision making, and growing stock option backdating scandals.

Other issues that have not received as much attention may be more important to the future of U.S. corporate governance and the competitiveness of U.S. markets. They include the growing demands for a convergence between the U.S. generally accepted accounting principles (GAAP) and the International Financial Reporting Standards (IFRS), which are being adopted in much of the world. U.S. GAAP is rules based and the IFRS is principles based. There are arguments as to the advantages of each system, but the whole world is moving away from the U.S. model. Any rules-based system should have rules that are simple to follow. The complexity of the U.S. tax system makes this very challenging.

The dual-tax system forces companies to have one version of the truth for regulators and another for federal, state, and even local tax authorities. According to *Compliance Week*, one-third of 400 material weaknesses declared in 2005 can be attributed, at least in part, to taxes. *Compliance Weekly* attributes this to the complexity of the dual reporting system and the myriad of jurisdictions in which companies must operate.

Adding to the misery, there is no harmony from one tax authority to the next, and SOX has resulted in the elimination of many tax shelters.[16]

Now back to the favorite whipping boy of corporate America—Section 404 of the Sarbanes-Oxley Act. One can make a very valid argument that most corruption and fraud and the marquee scandals of the past ten years had little to do with breakdowns in auditable internal controls. The most infamous scandal, Enron, was caused by accounting tricks in the use of off-balance-sheet entities, covered under Section 401. The current abuses of stock options fall under Section 403. One could also make a valid argument that the United States should take an approach more like the British model, which demands more from corporate boards.

The counterarguments in favor of Section 404 are also valid. As one who spent over 25 years cleaning up failures in internal controls, I realize there is a very strong argument that Section 404 only requires what well-run companies should have been doing anyway. Stronger internal controls typically translate into more automated and standardized controls, greater efficiencies, and lower operating costs. Well-run organizations understand this and have converted the negatives of greater internal controls into opportunities to clean up broken and disjointed processes, disparate systems, and inadequate controls.

We offer one last suggestion to address the heavy burden placed on small to midsize companies by internal control requirements of Section 404. There

are legitimate fears that Sarbanes-Oxley will hurt entrepreneurship by creating barriers for smaller companies to go public and access equity capital. Of course, the counterargument is also valid that many companies that went public in the 1990s lacked adequate internal controls and ultimately hurt investors. Some have called for a separate exchange for the little guys who cannot or choose not to comply with the internal control provisions of Sarbanes-Oxley. There may be a better approach. It would consist of a simple letter rating and grading system. The letter grade would appear next to the stock's symbol everywhere it is displayed. Even the most casual investors could then easily decide if they wanted to invest in more risky companies or go with companies that have demonstrated a strong track record of internal controls. It would look something like this:

A: Company passed 404 with a clean bill of health—no material weaknesses in the past four quarters.
B: Company conducted 404 attestation but with one material weakness in the past four quarters.
C: Company conducted 404 attestation with two material weaknesses in the past four quarters.
D: Company conducted 404 attestation with three or more material weaknesses in the past four quarters.
F: Company has restated earnings in the past four quarters.
X: Company has declined to go through the 404 attestation process.

Notes

1. Holly J. Gregory, "The U.S. Corporate Governance Experience," Forum for US-EU Legal Economic Affairs, Sponsored by the Mentor Group (Rome), September 13, 2001.
2. Holly J. Gregory, "Corporate Governance in the Global System," 2001.
3. Institute of Management Accountants, "Letter to the SEC: SEC File No. S7-24-06 and PCAOB Rulemaking Docket No. 021," February 13, 2007.
4. World Bank, "Comparison within One Country for All Six Governance Indicators," http://info.worldbank.org/governance/kkz2005/sc_country.asp.
5. World Bank, "Comparison for One Governance Indicator across a Number of Countries," http://info.worldbank.org/governance/kkz2005/mc_indicator.asp.
6. In our first book, *Manager's Guide to Compliance*, we devote a chapter on Australia's ASX-10 Principles as a best practice in corporate governance.
7. Lauren Etter, "Is Wall Street Losing Its Competitive Edge?," *Main Event*, December 2, 2006.
8. Oxera Consulting, "The Cost of Capital: An International Comparison," commissioned by the City of London Corporation, June 2006, www.oxera.com.
9. Ibid.
10. Becky Bright, "Many Lack Confidence in Efforts to Improve Corporate Governance," *Wall Street Journal*, October 9, 2006, R2.
11. Ibid.

12. Randal C. Picker, "The Legal Infrastructure of Business," Chicago Graduate School of Business, SB 42201, Fall 2006.
13. Hannah Clark, "CEO Compensation: Six Ways CEOs Hide Their Pay," *Forbes*, April 20, 2006.
14. Erin White and Aaron O. Patrick, "Shareholders Push for Vote on Executive Pay," *Wall Street Journal*, February 26, 2007, B1.
15. Martin Lipton, Wachtell, Lipton, Rosen & Katz, "What Directors Can Expect in the New Year," *Compliance Week*, January 3, 2006.
16. Tammy Whitehouse, "Taxes: A Fractured Control System," *Compliance Week*, October 3, 2006.

CHAPTER 67

SARBANES-OXLEY ACT

Sanjay Anand

After reading this chapter, you will be able to:

- Understand the key principles of the Sarbanes-Oxley Act (SOX)
- Understand the difference between principles-based and rules-based legislation, and the importance of each
- Understand the general requirements of SOX compliance
- Understand the benefits of complying with SOX regulations
- Understand the consequences of not achieving SOX compliance
- Understand the general corporate perceptions of SOX

67.1 INTRODUCTION

With the background understanding of where SOX came from and the circumstances that led to its inception, it is time to delve into the Act itself. This chapter

explains the concepts involved in the Act, including its key principles and the issues surrounding compliance.

This chapter will also discuss two important SOX-related organizations: the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB). These organizations play a vital role in the development and enforcement of SOX regulations, and understanding their functions is integral to understanding the Act itself.

67.2 KEY PRINCIPLES OF SOX

After investor trust was shaken by corporate scandal, it became clear that some key principles of behavior were missing from the governance strategies of at least a few publicly traded companies. An image of ethical behavior and respect for shareholder money is a vital component of U.S. markets; without it, investment could wane, and the economy would be significantly impacted.

SOX is designed to reassure shareholders that their investments are being protected from scandal and deception. To this end, the Act sets forth guidelines that compel companies to provide investors with all of the information that they require to make sound investing decisions.

The damaging effects of past investor cheating can be rectified in the minds of investors only if companies portray a consistent and unified commitment to honesty and fairness. That is why SOX was written with the spirit of three key principles: integrity, reliability, and accountability. (See Exhibit 67.1.)

(a) INTEGRITY. The Act seeks to instill integrity into publicly traded companies in both senses of the word. It is vital to maintaining investor trust that companies convey an image of high moral and professional standards. The goal is that, in time, investors will forgive past transgressions and recover their faith in the companies they invest in.

SOX also seeks to ensure the integrity of financial records in the sense that they are complete and representative. By requiring companies to present all relevant financial information, without exception, SOX aims to eliminate fraudulent and erroneous reporting.

(b) RELIABILITY. In addition to data integrity, SOX also seeks to ensure that the information that is reported is reliable and accurate. In the past, as companies were left to determine their own security levels, investors were without a clear benchmark standard or way of comparing security measures.

By establishing a standard that is applied across the board, SOX seeks to create a system in which corrupt and misleading behaviors are prevented and detected. This provides investors with assurance that security measures are in place to protect the accuracy of the information that they receive, thereby protecting their investments.

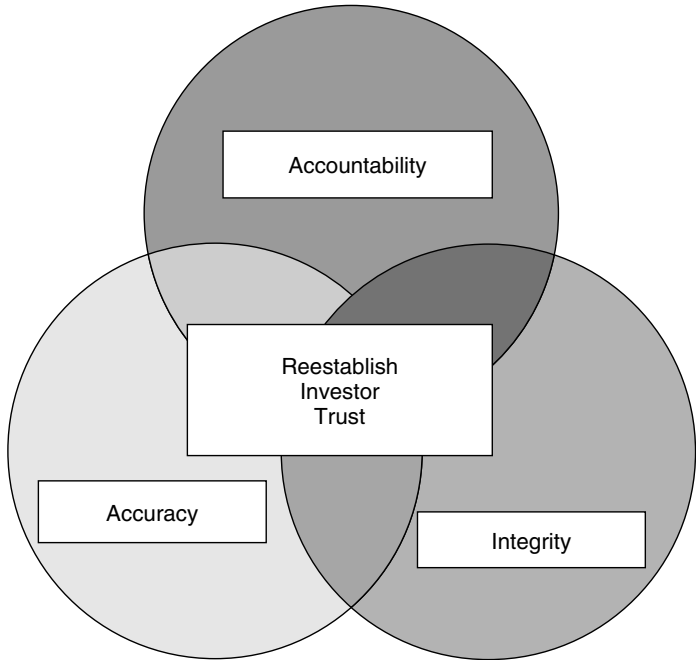


EXHIBIT 67.1 THREE PRINCIPLES: ACCOUNTABILITY, ACCURACY, AND INTEGRITY

(c) ACCOUNTABILITY. A common theme in corporate scandals of the past has been the elusive nature of the blamable party. It has seemed that within corporations, no members are culpable for the frauds, but rather the system creates an environment where blame can be passed on and ignorance can be claimed.

SOX seeks to ensure that when fraudulent or misleading material is released to investors there is a direct source for culpability and that one or more parties will be held accountable.

Through this Act, corporate executives and others responsible for financial reporting are answerable for breaches of information integrity and reliability. The motivation behind this principle is to eliminate the image of the faceless corporation and present both companies and the public with clear indications of which position is responsible for specific information and information-related tasks.

67.3 PRINCIPLES- AND RULES-BASED LEGISLATION

Looking back over history there is a cyclical trend between principles- and rules-based legislation governing corporations and their accountants. For example, the generally accepted accounting principles (GAAP) that emerged in the 1930s are the result of principles-based regulation. These principles reflect self-regulation,

as GAAP was created by accountants for accountants. The nature of self-regulation such as this is beneficial because it means that the principles are readily applicable and that there is not the same growing stage as is seen when outsiders attempt to create rules for an industry.

Those who support principles-based legislation also argue that it provides freedom and flexibility for those applying it, while still enforcing codes to govern activities. Although this flexibility does provide benefits, such as the ability for the legislation to grow and advance with changes in the industry, it also has its drawbacks.

Returning to the GAAP example, the self-regulation and flexibility found here has resulted in some negative effects regarding conflicts of interest. It is reasonable to suspect that an industry will not have a clear perspective on how best to regulate themselves and that temptations or nearsightedness could lead to insufficiencies.

Those who feel that principles-based legislation has challenges would argue that accounting principles are not sufficient to prevent undesirable activities; for example, many of the actions taken during the Enron scandal were in fact consistent with GAAP.

Unlike principles-based legislation, rules-based legislation does not provide the same flexibility or self-regulation, meaning that it is more rigid and less vulnerable to conflicts of interest. However, rules-based legislation does have a steeper learning curve and it can take longer before an industry is effectively able to adapt to the regulations.

For example, SOX has been designed to provide specific rules for auditors to directly prevent misrepresentation of financial information. The difficulty is that these rules have been laid out without instructions about how companies are to comply. It is from this lack of guidance that many SOX compliance issues have arisen.

Given the pros and cons of both principles- and rules-based legislation, there appears to be a solution in layering the two. By providing companies and auditors with the rules found in SOX, but providing guidance through a series of principles such as GAAP and the auditing standards, a combination of rigid regulations and effective, flexible implementation can be achieved.

67.4 SOX COMPLIANCE

SOX mandates that its provisions be complied with by all companies in the United States that are publicly traded. This also includes those companies that are initiating their initial public offerings (IPOs).

Additionally, SOX compliance is required of foreign companies under certain circumstances. One instance is in the case that a company exists outside of the United States, but is a wholly owned subsidiary of a U.S. corporation. Non-U.S. companies that are publicly traded on U.S. markets through American depositary receipts (ADRs) are also required to comply.

67.5 GENERAL COMPLIANCE REQUIREMENTS

To say that a company has achieved SOX compliance is largely to say that they have taken the necessary steps toward assuring the public of the accuracy of their financial reports. Such a distinction is meant to reassure investors that the information that they receive from this company is valid and truthful.

In keeping with the three key principles of the Act, which are integrity, accuracy, and accountability, SOX compliance seeks to regulate companies and their reporting activities. Compliance with SOX requires the company release all relevant financial data to ensure the integrity of the information. It also requires that the data that is released is reliable to ensure its accuracy. Finally, it mandates that the CEO and CFO verify the data and accept accountability for any errors.

In order to ensure that financial reporting practices are accurate, SOX requires that companies establish and maintain an accounting framework that includes internal controls. These controls are designed to secure the financial documents from error and misrepresentation, thereby protecting those who rely on the documents' accuracy.

To this end, SOX compliance also requires that company executives assume responsibility for the establishment and maintenance of that framework.

(a) ASKING PRIVATELY HELD COMPANIES TO ACHIEVE SOX COMPLIANCE. Although privately held companies are not legally compelled to comply with SOX standards, they are likely to feel market pressure to do so. SOX and its regulations are designed to benefit company shareholders by protecting their interests and ensuring that they receive complete and accurate information. In doing so, SOX allows shareholders to remain confident that they are basing their investment decisions on truthful information and they are not being deceived in any way.

It is reasonable to expect that industry regulators, lenders, insurers, government entities, and accountants who deal with private companies will encourage SOX-like compliance through their desire for similar benefits.

Although such compliance efforts would not be enforceable through the PCAOB, there is no stipulation that would prevent financial institutions from requiring SOX compliance as a component of their contract requirements.

(b) STEPS PRIVATELY HELD COMPANIES CAN TAKE TOWARD VOLUNTARY SOX COMPLIANCE. It is widely understood that SOX has been designed to protect the interests of the shareholders rather than those of the companies. The regulations and requirements of SOX compliance work to ensure that shareholders receive only accurate information and that their investments are not threatened by data errors or misrepresentations.

Although not compelled to comply by the PCAOB or any other regulatory board, private companies may opt to achieve voluntary SOX compliance in order to offer their investors similar benefits and boost their images.

The following are steps that privately held companies can take toward achieving voluntary SOX compliance. (See Exhibit 67.2.)

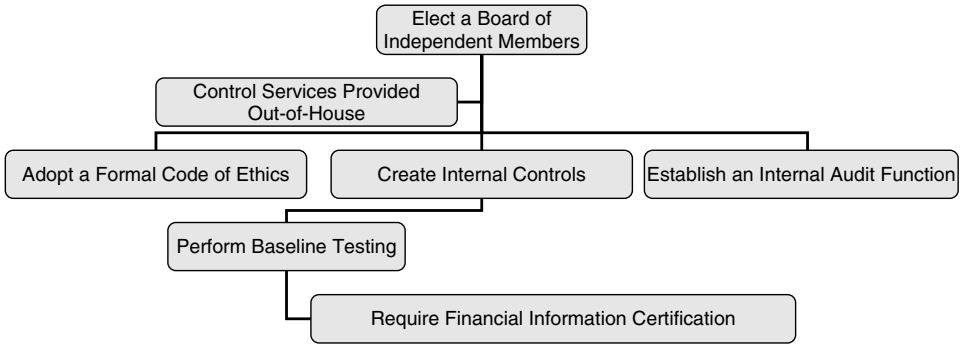


EXHIBIT 67.2 STEPS TO INITIATE SOX COMPLIANCE

1. Elect a board of independent members.
   Even if there is just one, independent board member(s) serve useful evaluation functions within a company and can function as the foundation for a future audit committee.
2. Create internal controls and perform baseline testing.
   Doing so will enable the company to establish operational benchmarks and create an organizational framework for further compliance.
3. Adopt a formal code of business conduct and ethics.
   Separate codes can be established for varying levels within the company that offer guidance specific to job descriptions.
4. Establish an internal audit function.
   Whether through hiring a consultant or establishing a new position, the company can monitor and evaluate internal controls by establishing an internal audit function.
5. Require financial information certification.
   Certifying financial information leads to enhancements in internal accounting competencies.
6. Control services provided by outside accounting firms and auditors.
   By limiting the risk of external accountants providing conflicting services, companies will minimize problems with state regulators.

67.6 BENEFITS OF COMPLIANCE

There are those companies that, regardless of whether they support SOX in general, have embraced the compliance efforts and even their associated costs as investments in their future. These companies view SOX regulations as standards that will improve their companies' organization and facilitate their ability to control finances.

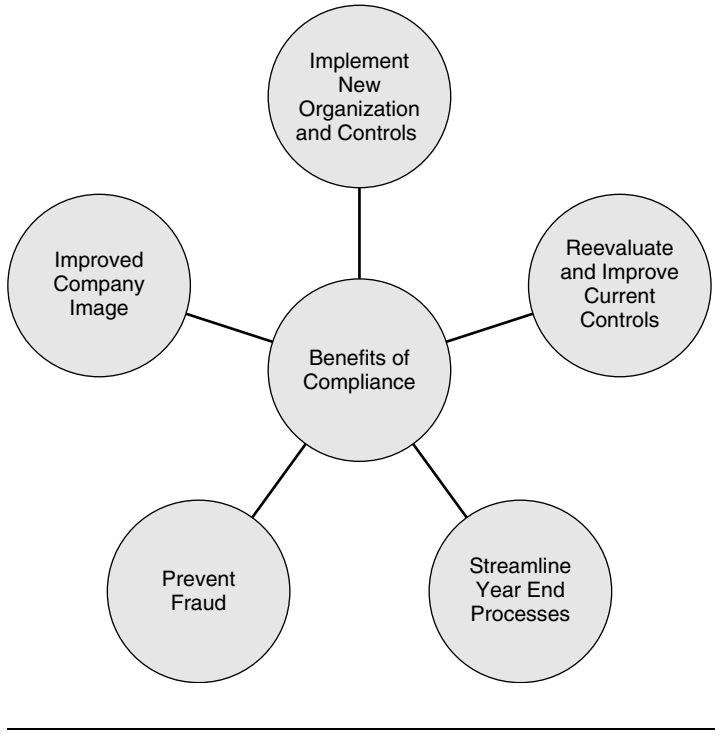


EXHIBIT 67.3 MAJOR BENEFITS OF COMPLIANCE

Some of the benefits of SOX compliance that can provide financial reward in the end are shown in Exhibit 67.3. They include:

- Encouragement to organize and develop controls

  Many companies recognize the importance of establishing solid internal controls, but find that it never seems to reach the top of their priority list. By mandating such actions, SOX forces companies to evaluate operations and establish a comprehensive framework of controls. As a result, the executive, board, audit committee, and management will be able to gain control over all aspects of operations, improving productivity and minimizing risks.
- Encouragement to reevaluate and monitor current controls

  Through their efforts to comply with SOX, companies are forced to document and reevaluate already-established controls. Through this reevaluation, these companies can identify controls that have not been properly maintained and updated. By combining reevaluation of old controls with the redesign of new ones, companies are able to create a comprehensive system in a cost-efficient manner.
- More organized year-end process

  Because SOX compliance forces companies to develop and integrate systems for document organization, it also keeps their financial records

up to date and easily accessible. This additional attention and control in maintaining financial data and documents facilitates greater efficiency and higher organization during the year-end process of SOX-compliant companies, thereby decreasing the costs and time associated with this.

- Prevention of fraud

  Finally, one of the greatest benefits of SOX is that it establishes requirements that are ultimately designed to protect from fraud. The increased security and antifraud protections required by SOX benefit companies by preventing the fates experienced by Enron and other companies that suffered under scandal and went bankrupt as a result.

67.7 CONSEQUENCES OF NONCOMPLIANCE

Non-compliance with SOX falls directly upon the shoulders of the executive officers who are required to certify the accuracy and integrity of the company's financial reports. In addition to civil lawsuits and damage to market image, CEOs and CFOs of companies that are noncompliant with SOX are subject to financial penalties and potential incarceration.

Situations where willful deceit cannot be proven carry fines of up to $1 million and ten years in prison. However, in the event that wrongful certification has been submitted intentionally, the penalty maximum rises to $5 million and 20 years in prison.

(a) WHO ELSE IS AFFECTED? SOX's primary objective is to protect those investors who purchase stocks on the U.S. markets, whether those investors are U.S. citizens or foreign purchasers.

Although SOX primarily targets publicly traded companies that are listed on the U.S. markets, it also presents significant implications that both directly and indirectly affect privately owned companies as well.

SOX contains provisions that affect document retention, criminal fraud, and aspects related to the Employee Retirement Income Security Act (ERISA); these are issues that are relevant to both privately and publicly owned companies.

Moreover, any privately held company that seeks venture capital funding, commercial loans, or initial public offerings (IPOs), or that will conduct significant business with a publicly traded company will be directly affected by SOX.

Although many will try to extrapolate SOX to make it applicable to private companies, that is not the intention of the Act. SOX was written to protect investors; however, the regulations and provisions within the Act can be seen as a standard for financial reporting efforts in any company.

In cases where loan granters and other organizations require SOX compliance of private companies through their contracts, these requirements are not PCAOB related and not enforceable by their standards.

67.8 VOLUNTARY VERSUS MANDATORY COMPLIANCE

Since the passing of SOX, a great deal of philosophical and practical debate has been generated regarding whether corporate governance should be voluntary or mandatory. Those in favor of eliminating mandatory compliance and abolishing regulations such as SOX argue that companies have enough market incentive to adopt corporate governance policies voluntarily without the oversight of organizations such as the PCAOB.

Proponents of voluntary compliance argue against mandatory regulations, citing inefficiencies associated with broadly termed and widely scoped regulations. Pointing to high costs associated with SOX compliance, they argue that voluntary compliance would eliminate redundancy and allow companies to comply with only those regulations that directly apply to their operations.

They also argue that organizations such as the PCAOB are unnecessary evils that create further financial burden on companies through their fees, money that could be spent on greater controls.

However, those in favor of mandatory compliance cite the fact that such regulations improve the public's ability to make informed decisions regarding investments, thereby improving market activities and generating further revenue for publicly traded companies.

Supporters of SOX and similar regulations also cite historical corruptions as proof that voluntary compliance is ineffective. They argue that given the freedom to govern themselves, many companies will ignore the dangers associated with inadequate controls and will leave themselves and their investors open to deception in order to cut costs.

A third camp believes in the development of a compromise. Such a compromise could be a partially mandatory structure in which some SOX-like regulations would be enforced and others would be voluntary.

One reconciliation that has been suggested is to propose recommendations, similar to those contained in SOX, for which compliance is voluntary, but mandate that companies disclose which recommendations they have complied with and how.

This system of voluntary compliance and mandatory disclosure would provide investors with the information that they require and create greater market pressure toward compliance through competition over investment funds.

Irrespective of which camp is correct, there is no indication that SOX will be going anywhere soon. It seems it is here to stay.

67.9 CORPORATE PERCEPTIONS OF SOX

When SOX was passed, there was a consensus among the public, the government, and commercial leaders that some sort of action was required to prevent corporate scandals from continuing to erode the integrity of U.S. markets.

Although there still appears to be a general consensus that action is required to remedy the corporate landscape of corruption and reinstate public trust,

there is a great deal of dissent regarding the specific actions taken by the government.

Several companies, accounting firms, and lobbyist groups have lodged various arguments against SOX and its enforcement. Two of the greatest complaints relate to the cost of compliance and the impact that the Act has on small businesses.

Although SOX is a controversial Act that has created divided opinions regarding its necessity, fundamentals, and implementation, there are compliance benefits that improve the functioning of participating companies. Those organizations that choose to focus on these benefits will find that they have a much easier time accepting SOX and driving their compliance efforts forward.

67.10 CONCLUSION

The Sarbanes-Oxley Act (SOX), and everything related to its enactment, is based on three core principles: integrity, accountability, and accuracy. Essentially, these are the three principles that appeared to be lacking in those companies that have experienced corruption and fraud. The importance here is that shareholders and the general public are able to trust that financial records will be complete and will provide true information. It is also important that if error or misrepresentation occurs, there is an established system in place to hold culprits accountable.

There are two types of regulations that are applicable to corporations; they are principles- and rules-based legislation. Principles-based legislation offers flexibility and greater ease of application, while rules-based provides more rigid regulations and greater external control. Each has its pros and cons, and there is room for both within a greater framework of governance. For example, GAAP and SOX are able to work together for overall protection that is both feasible and enforceable.

The greatest action associated with SOX is the achievement of compliance. To comply with the Act means that the company has taken the necessary measures to pass its SOX audits and has been identified as a company that provides accurate financial information.

When companies achieve compliance, they not only provide their shareholders with greater security, they also provide themselves with several financial rewards. These rewards include the benefits of greater system efficiency, less loss due to error, greater ease filing taxes, and less risk of fraud.

67.11 SUMMARY

The three core principles of SOX are accountability, accuracy, and integrity.

- SOX seeks to provide rules-based legislation to fill the gaps that principles-based regulation cannot fill.

- SOX compliance requires that the company takes all necessary steps to ensure that its financial reports are accurate and complete.
- SOX mandates that CEOs and CFOs certify the accuracy of all financial reports, as well as verify the efficacy of the controls that offer security to financial reporting systems.

INDEX

CHAPTER 68

MEASURING THE EFFECTIVENESS AND PERFORMANCE OF YOUR GOVERNANCE, OPERATIONAL RISK, AND COMPLIANCE PROGRAMS

Scott L. Mitchell
Carole S. Switzer, Esq.

Managing operational risk in the current era of enforcement, shareholder suits, and explosive class action activity poses huge risks if you fail—and presents game-changing opportunities if you choose to embrace it.[1] Over the past few years, organizations have focused a lot of time, energy, and resources on designing, implementing, and improving governance, operational risk, and compliance (GRC) programs to address operational risks. Some executives are appropriately asking, "Is all of this work really working? Are we actually and factually delivering outcomes that really matter?"

While the art, science, and practice of program evaluation are still in their infancy, there are several sound practices that organizations of all sizes can use to get answers to these questions. As we approach program evaluation, it is important to remember that managing governance, risk, and compliance (GRC) is fundamentally similar to—*not* fundamentally different from—other enterprise processes. As such, we can use tried-and-true techniques to evaluate our approach.

So, with all of that said, what should we evaluate? What are the goals of the evaluation? How should we do it?

Generally speaking, there are two types of evaluations that you should consider: effectiveness evaluation and performance evaluation. The former helps an organization meet minimum requirements and receive credit for putting in place a program that is logically designed using sound practices. The latter helps an organization understand if the program is truly delivering business benefits and where investments can be optimized.

In the world of compliance and internal control, *effectiveness* is a term of art that has specific meaning. (See Exhibit 68.1.) Although legal compliance (including issues associated with preventing and detecting fraud) represents a subset of the issues typically included in operational risk, it is important that organizations use this common denominator when evaluating the program. For it is this definition that will be used by enforcement and justice when (not if) things go afoul.

It is important that we, as practitioners, accept this definition—and not attempt to expand it. Doing so only invites regulatory uncertainty and confusion. And, most important, redefining "program effectiveness" is unnecessary, as most practitioners will find more value in using "program performance" as a more powerful concept.

Performance brings into view the totality of the program and determines if it is delivering real business value. This concept certainly includes effectiveness, as a solid program must meet the minimum legal requirements. However, as most executives know, performance helps an organization dig into the issues that matter most and answer, "Is our program delivering business value? Where should we focus our time and resources to make it better?"

68.1 TAKING A STEP BACK

To elaborate on program evaluation, one must take a step back and consider goals of organizational performance. At the highest level, all organizations are in

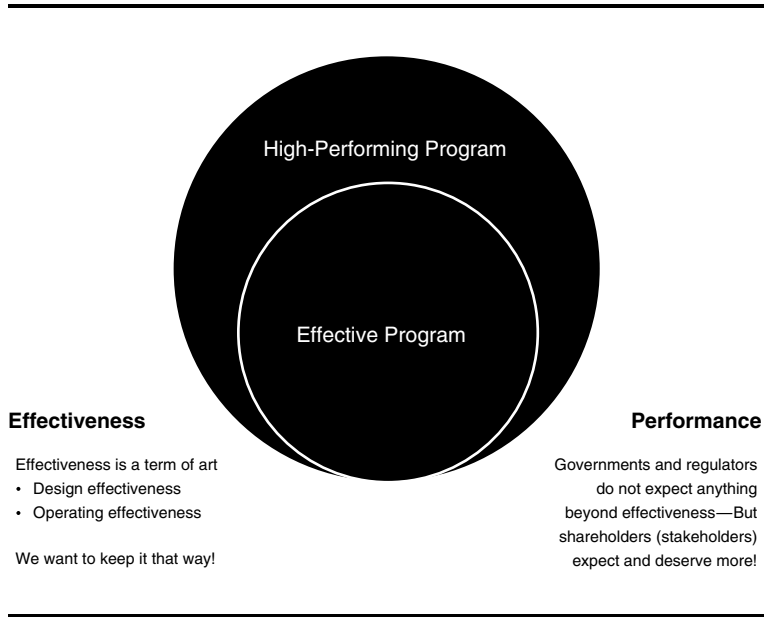


EXHIBIT 68.1 DIMENSIONS OF EVALUATION

business to achieve objectives while staying within boundaries of conduct. (See Exhibit 68.2.)

To do this:

- The organization must set clear *objectives* that define why it exists and what it seeks to achieve.
- The organization must establish a *business model* designed to achieve its objectives. The board oversees the objective-setting process, the business model, and performance reporting. Management executes strategy and operates the business model.
- The organization must operate within defined *mandated boundaries*. Outside forces such as legal and regulatory requirements establish these mandated boundaries.
- Similarly, the organization must operate with defined *voluntary boundaries*. Management determines the organization's voluntary boundaries, which include items such as public socioeconomic commitments, standards certifications, contractual and representational obligations (i.e., warranties, guarantees, etc.), and organizational ethics and values. It is important to treat voluntary boundaries just as seriously as the mandated ones, because violations of either can carry equally significant adverse consequences.
- In the course of conducting business operations, the organization must understand both the internal and external obstacles that may get in the way of achieving its objectives, and recognize the opportunities that may

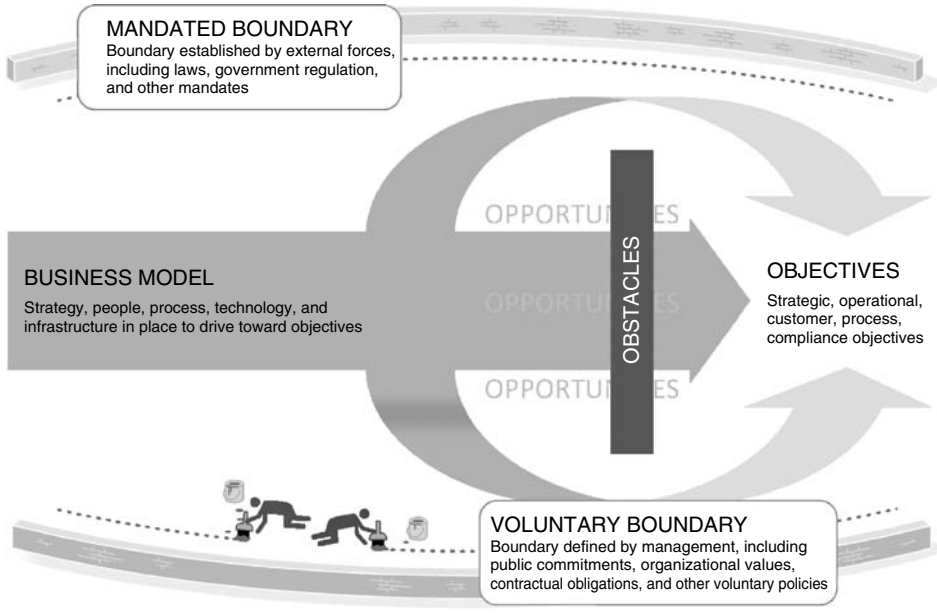


EXHIBIT 68.2 BIG PICTURE OF ORGANIZATIONAL PERFORMANCE

transform either the objectives themselves or the business model to achieve the objectives.

An organization must be adept at operating within boundaries, overcoming obstacles (or preventing them from undermining its efforts), and seizing upon opportunities to attain its business objectives.

The governance, risk, and compliance approach (and the various programs and capabilities that are a part of the overall approach) fits into this picture by providing a capability to identify the boundaries and obstacles and establishing a system to let management know when it is getting close to (or crossing) a boundary or approaching an obstacle. Once such a situation is detected, management must respond quickly and appropriately to minimize the impact on the organization. As issues are encountered and addressed, management should also continuously improve the program to reduce the likelihood that prior issues resurface, similar issues materialize, and new issues arise unexpectedly. Additionally, whether old or new, management should improve program responsiveness, prevention, and detection, so issues do not impact the organization to the same degree in the future.

So the question is whether the GRC approach and all of the component programs and capabilities are delivering business value.

68.2 PROGRAM EFFECTIVENESS

Let us begin with the basis of all evaluation. "Effectiveness" looks at whether the program is logically designed (design effectiveness) to address all mandated and voluntary requirements, and whether the program is actually operating as designed (operating effectiveness). In this sense, the evaluation helps to determine if the program is delivering required legal and regulatory outcomes and appropriately reflecting the voluntary promises that the organization has made with regard to how it approaches governance, risk, and compliance.

(a) MANDATED BOUNDARIES. Initially you will want to show that the program's design incorporates criteria that are explicitly delineated by mandated or de facto mandated sources. U.S. examples would include:

All Organizations

- Federal Sentencing Guidelines for Organizations
- Criteria outlined in the Holder/Thompson/McNulty Memoranda
- Criteria outlined in the Caremark commentary

Publicly Traded Organizations

- *Seaboard* Report
- Listing requirements

Beyond these general mandates that require all organizations to conduct some level of risk assessment and management, there are numerous industry mandates, especially in highly regulated industries such as banking, financial services, and life sciences. These industry mandates often prescribe specific techniques and formulas that must be applied to managing governance, risk, and compliance.

In addition to the mandates about how the program itself should be designed, there are specific mandates that apply to the organization that the program must be prepared to address. For example, for legal compliance, most programs should be prepared to address:

- Governance requirements
- Fraud and corruption prevention
- Employment and labor issues
- Environmental issues
- Health and safety issues
- Information management issues (security, privacy, intellectual property issues, etc.)
- Competitive practices (antitrust, fair advertising, etc.)
- Government interactions (government contracting, lobbying, etc.)

The key point is this: For all of the discussion about the danger of "ticking boxes" it is critical that these legally mandated structures and practices are

in place. While the mere presence of these structures and practices does not ensure a high-performing program, they help to generate an important outcome—protection. Being able to prove that these structures and practices are in place will help protect the organization when (not if) it finds itself explaining to enforcement agencies or other stakeholders why an adverse event occurred and why it was not prevented.

(b) VOLUNTARY BOUNDARIES. Beyond the legal (and semilegal) mandates, organizations must also identify the voluntary boundaries that it has set for itself via explicit or implicit promises and agreements:

- Commitment to a specific risk management framework (e.g., COSO ERM, Australian standard)
- Commitment to nonmandated industry best practices (e.g., PhRMA Code in life sciences)
- Commitments to specific ratings agencies about how they will address risk (e.g., Standard & Poor's, Fitch, GovernanceMetrics, etc.)
- Commitments to specific core values and representations about the brand (e.g., if the organization is serious about developing a culture of open communication, there should be specific elements in the program designed to meet this commitment)
- Commitments to corporate social responsibility and sustainability practices
- Commitments to customers and partners about how the organization identifies and addresses risk

There are a number of other voluntary commitments that an organization may make about its program. The key is to understand what these explicit or implicit promises are so that you can ensure that the program addresses them in some way.

(c) CONDUCTING THE EFFECTIVENESS EVALUATION. Once the mandated and voluntary boundaries for the program are understood, management should conduct an evaluation of the design and operating effectiveness.

- Design effectiveness evaluation is similar to a gap analysis. For each mandated requirement and voluntary commitment, management should ensure that there is at least some coverage. For example, the Federal Sentencing Guidelines for Organizations requires that an organization conduct a risk assessment that looks at both company and industry trends. Many practices can address this requirement. Management should make sure that something logical and reasonable is in place.
- Operating effectiveness evaluation tests to see if the structures and practices are actually working as designed. Operating effectiveness evaluation usually takes form in a series of periodic tests or via some reliable ongoing monitoring of operational data. For example, all organizations should

install a whistle-blower hotline so that stakeholders can notify (anonymously if desired) management of potential wrongdoing. The hotline will be designed to ensure that all of the protections are in place. However, it is critical that the hotline operate as designed. To do this, management should periodically enter fictitious issues into the system and observe whether the system works as designed.

68.3 BEYOND EFFECTIVENESS

Just because there is no legal requirement to go beyond effectiveness does not mean that you should not care. Shareholders and stakeholders are demanding more. And, at a practical level, neither design nor operating effectiveness will help management and the board judge performance or allocate scarce capital.

As well, and for better or worse, some enforcement agents and regulators may look for more than just rote design and operating effectiveness. Some U.S. attorneys have retained consultants to perform culture assessments and to evaluate other outcome measurements to help determine whether to prosecute an organization. While this may be considered as overreaching, it is a reality that all organizations must face.

So again, beyond design and operating effectiveness, in the current environment, shareholders, the board, management, and other stakeholders[2] are demanding more—they demand total program performance.

68.4 TOTAL PROGRAM PERFORMANCE

"Performance" looks not only at the effectiveness of the program, but also its efficiency, responsiveness, and the degree to which it delivers business outcomes that go beyond legal and regulatory requirements—outcomes that really matter to stakeholders. These dimensions are similar to the classic performance triangle of quality, cost, and speed, as shown in Exhibit 68.3.

For better or for worse, program performance is generally not considered by lawmakers and regulators. For example, regulators do not particularly care if a hotline costs $10,000 per year or $1 million per year to operate, as long as it is appropriately designed and operating as designed. With few exceptions, it does not matter if it takes one week or three weeks to process an issue through the system as long as the issue is reasonably and appropriately handled. And the presence of logically designed training that takes a certain amount of time to go through is more important to regulators than the actual knowledge transfer and outcome that it generates.[3]

And, frankly, this is the appropriate role of governments and regulators. Organizations and, ultimately, stakeholders would not be best served by having the government design business processes.

But just because the government doesn't (in most cases) care about performance, you should care. As with all enterprise processes, stakeholders demand

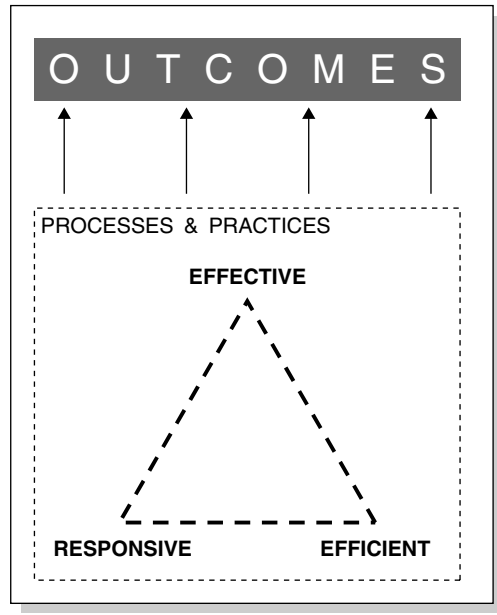


EXHIBIT 68.3 TRIANGLE OF QUALITY

that organizations are not only effective, but also efficient and responsive and deliver on enterprise objectives.

68.5 PERFORMANCE MEASUREMENT BENEFITS

There are numerous benefits and challenges to measuring the performance of a program. A well-known maxim is "what gets measured gets done; what gets rewarded gets repeated." The governance, risk, and compliance capability and approach is no different.

Ideally, performance measurement will help an *organization*:

- Demonstrate that the program meets minimum legal requirements (effectiveness)
- Demonstrate how program results support objectives and create or preserve value
- Highlight what works and what doesn't (improvement opportunities)
- Justify capital allocation
- Demonstrate accountability
- Motivate and provide tangible feedback to employees
- Enrich communications with stakeholders

For the *program*, measurement helps:

- Justify resource allocation
- Frame maturity targets
- Prioritize initiatives and projects
- Define advancement and career paths

For the *individuals* delivering on program objectives, measurement:

- Instills a goal-oriented mind-set
- Provides a basis for demonstrating personal success for reward and advancement
- Connects the individual's efforts into the broader picture
- Promotes understanding of expectations and job satisfaction

68.6 MEASUREMENT PRESENTS CHALLENGES

Measurement of the program will have to overcome a number of challenges associated with performance measurement, including:

- Unintended consequences
- Perception versus fact
- Long-term results
- Prevention and deterrence
- Multiple contributors
- Inconsistent or incompatible information

(a) UNINTENDED CONSEQUENCES. These can occur when inappropriate or perverse incentives or measures are put in place. In one professional services firm, contract compliance was historically measured in the first quarter of each year. When the firm switched to continuous monitoring of contract compliance, it found that contracts closed in the first quarter were five times as likely to comply with standard terms and conditions than contracts in the other three quarters. Knowing that the first quarter was all that really mattered led some (many) people to focus only on the first quarter when it came to contract compliance.

(b) PERCEPTION VERSUS FACT. Several program outcomes require measuring the perceptions of stakeholders, typically via surveys and ethnology. These tools do not necessarily indicate fact (e.g., a survey may ask employees if they have observed misconduct, and they may not have the appropriate knowledge to know if something is actually misconduct), but they do provide an adequate proxy for information. In some cases, the perception is the "fact" that management is looking to measure. For example, if employees perceive there is some type of misconduct going on in the organization (even if untrue), the perception is there and must be addressed in some manner, even if the underlying assumption is incorrect.

(c) LONG-TERM RESULTS. In some cases, the outcome of a program may not be realized for many years, which can make it difficult to obtain measurement data. For example, it may take several years to actually see that the implementation of a certain initiative (e.g., training program on fraud prevention) has helped to prevent, reduce, or detect incidents of fraud. In some cases, this can be addressed by identifying meaningful output-oriented milestones that lead to achieving the long-term outcome goal (e.g., keeping track of training data that will help with the long-term goal of reducing fraud in the workplace).

To address this issue, a program should define the specific short- and medium-term steps or milestones to accomplish the long-term outcome goal. A road map can identify these interim goals, suggest how they will be measured, and establish a schedule to assess their impact on the long-term goal. It is important that these steps are meaningful to the program, measurable, and linked to the outcome goal.

(d) PREVENTION AND DETERRENCE. By definition, a key outcome of the program is the deterrence or prevention of negative events. It is very difficult to prove a negative. Deterrence measurement requires consideration of what would happen in the absence of the program. It is often difficult to isolate the impact of the individual program element on any behavior that may be affected by multiple other factors.

For areas where noncompliance is not life-threatening and where compliance is historically low, a legitimate long-term target may fall short of 100 percent compliance. In these cases, short-term targets that demonstrate forward progress toward the acceptable long-range goal may make sense.

For areas where failure to prevent a negative outcome would be catastrophic (including programs to prevent life-threatening incidents), traditional outcome measurement might lead to an all-or-nothing goal. As long as the negative outcome is prevented, the program might be considered successful, regardless of the costs incurred in prevention or any close calls experienced that could have led to a catastrophic failure. This can be a dangerous and costly practice.

More appropriately, proxy measures can be used to determine how well the deterrence process is functioning. These proxy measures should be closely tied to the outcome, and the program should be able to demonstrate—such as through the use of modeling and/or factor and correlation analysis—how the proxies tie to the eventual outcome. Because failure to prevent a negative outcome is catastrophic, it may be necessary to have a number of proxy measures to help ensure that sufficient safeguards are in place. Failure in one of the proxy measures would not lead, in itself, to catastrophic failure of the program as a whole; however, failure in any one of the safeguards would be indicative of the risk of an overall failure.

(e) MULTIPLE CONTRIBUTORS. Often several business processes and capabilities contribute to achieving the same goal. The contribution of any one program may be difficult to measure. One approach to this situation is to develop broad,

yet measurable, outcome goals for the collection of programs, while also having program-specific performance goals.

One example of this is culture. Ideally, the program will help to develop an environment of trust, accountability, and integrity. This in turn will contribute to talent attraction, talent retention, and talent satisfaction.

That said, it is difficult to prove that the program is the *only* contributor to those outcomes. Nevertheless, management should collaborate to better understand how the full complement of processes and programs (human resource processes, evaluation processes, compliance and ethics processes, etc.) work together to achieve desired outcomes—and, if appropriate, assign some value to the contribution of the program.

(f) INCONSISTENT OR INCOMPATIBLE INFORMATION. Data may be inconsistent or incompatible across the enterprises, and apples are not always compared to apples. For instance, the methodology used to evaluate information privacy risks may be completely different than the methodology used for employment compliance. This is especially true when analyzing information from more than one organization. Extra care should be given to normalizing data so that accurate analysis can be conducted.

68.7 MEASURING PROGRAM PERFORMANCE

The measurement planning process defines the overall measurement strategy, approach, required resources, and information. These activities are conducted periodically to ensure that what you are measuring remains salient to both the program and its role in the organization.[4]

- Identify and review business objectives.
- Identify program objectives that are aligned with enterprise objectives.
- Define indicators and targets to measure performance.
- Measure indicators.
- Analyze indicators.
- Improve and control program processes to drive indicators toward targets.

(a) BUSINESS OBJECTIVES: START WITH THE END IN MIND. While each organization may pursue unique enterprise objectives, most pursue objectives that fit within these themes:

- Growth
- Profitability
- Return or spread: return on invested capital (ROIC), return on equity (ROE), total return, return on invested capital minus weighted average cost of capital (ROIC – WACC)
- Future value (the value that the market puts on the potential for future growth and profitability reflected in share price)

These business outcomes are typically enabled by key performance drivers such as:

- Brand/reputation
- Workforce productivity
- Quality
- Customers (acquisition, retention, loyalty, engagement, etc.)
- Innovation

Again, organizations will have their own unique set of enterprise objectives. The key is to clearly understand both the objectives and how those objectives are measured so that program objectives can be aligned to these overall enterprise objectives and measures can be consistent with, or at least correlated to, enterprise measures. For example, if an organization is focused on growth and new markets, a GRC professional should focus on how the program helps to improve risk-adjusted revenue in emerging markets where fraud and corruption may be more frequent. If an organization is focused on profitability, demonstrate how investments in the program will break down compliance silos and reduce overall transaction costs over five years. If an organization is focused on attracting and retaining talent, demonstrate how the program contributes to key workforce drivers, such as an open environment and clear accountability.

(b) IDENTIFY AND ALIGN PROGRAM OUTCOMES/OBJECTIVES. Management must take these enterprise objectives and define appropriate program objectives. As with enterprise objectives, every program is unique and, thus, will pursue unique objectives. (See Exhibit 68.4.) That said, there are a few universal program objectives that most organizations strive to attain. Ultimately, a program should accomplish 10 things:[5]

1. Inspire a culture of performance, accountability, trust, and open communication
2. Prevent noncompliance and unethical conduct
3. Prepare for actual or perceived noncompliance and unethical conduct
4. Protect the organization from negative consequences
5. Detect noncompliance, control weaknesses, and undesirable shifts in culture
6. Respond to noncompliance, control weaknesses, and undesirable shifts in culture
7. Improve the program to better prevent, prepare, protect, detect, and respond
8. Reduce loss due to noncompliance and unethical conduct
9. Optimize costs to sustain the program
10. Enhance stakeholder perception of organizational value

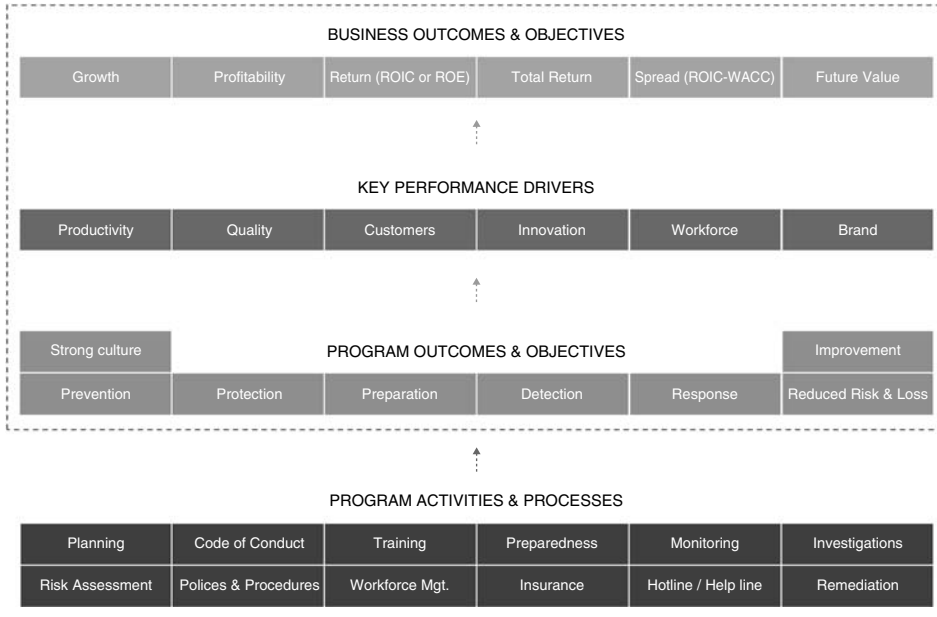


EXHIBIT 68.4 ALIGNMENT OF ORGANIZATIONAL OBJECTIVES, VALUE DRIVERS, AND PROGRAM OBJECTIVES

These universal program outcomes and the indicators used to measure progress toward them are discussed in greater detail later.

Align Program Outcomes with Business Objectives[6]

Enterprise Strategy	Objectives	Program Contribution
Growth	Deepen relationship with customers	Improved brand reputation via reduced risk (or actual incidents) of noncompliance
	Develop new markets	Reduced revenue risk in new and emerging markets (anticorruption program)
	Access additional sources of capital	Reduced compliance and ethics risk that is measurable and able to be communicated to investors and lenders

Enterprise Strategy	Objectives	Program Contribution
		Focus on specific risk areas (e.g., environment, labor relations) provides access to socially responsible investors
Profitability	Reduce transaction costs	Reduced costs of manual compliance processes
	Reduce duplication	Common people, processes, and technology in various compliance silos are streamlined
	Reduce errors	Reduced rework associated with mishandled forms and filings
		Reduced fines, penalties, and costs associated with innocent noncompliance
	Reduce pernicious conduct	Reduced fines, penalties, and costs associated with willful noncompliance
	Improve legal protection	Reduced operational risk that is measurable and managed
Workforce Performance	Improve productivity	Improved culture of alignment, openness, trust, and accountability are key ingredients to high workforce performance
	Become employer of choice	Improved culture contributes to positive employee perceptions about the organization as a whole
		Improved culture contributes to reduced sick days
Brand/Reputation	Improve reputation with regulators, investors, media, community, suppliers, employees, and customers	Reduced operational risk that is measurable and able to be communicated to stakeholders (Also see ''Profitability'' above, as many areas contribute to brand/reputation)
	Improve asset security (information security)	Reduced vulnerability to both innocent and pernicious leaks of customer, partner, and employee information

(c) DEFINE INDICATORS AND TARGETS. Once you understand what you are trying to accomplish with the program and how it links to enterprise performance, you should define indicators that will help you evaluate the performance of the program that can be linked or correlated to the indicators and targets used to measure the business objectives. Candidate indicators are provided at the end of this chapter (See Exhibit 68.5).

The following criteria and questions are helpful in defining performance indicators. Indicators should be specific/simple, measurable, actionable, relevant, and timely (SMART):

Metric
A quantitative measure {PRIVATE} of the degree to which a system, component, or process possesses a given attribute.

Indicator
A single metric or combination of metrics that provide insight into a process, practice, or outcome to enable assessment and improvement. Indicators are either leading (predicting the future) or lagging (documenting the past).

SPECIFIC/SIMPLE

- Is it clear exactly what is being measured?
- Is it easily understood?
- Would two different people measure it in the same way?
- Does the indicator isolate the true event?
- Does the indicator avoid mixed messages?

MEASURABLE

- Can it be quantified?
- Is it accessible and worth the cost to obtain the data?

ACTIONABLE

- Once we understand the value of the indicator and any trends, will it be possible for us to take meaningful action?
- Are the underlying processes that can affect this indicator under our control?

RELEVANT

- Will tracking this indicator drive the appropriate behavior—or generate unintended consequences?
- Does the indicator capture the essence of the desired outcome?

TIMELY

- Can it be frequently updated?
- Will the indicator reveal itself in time to take appropriate action?

Be sensible and practical in applying these criteria. No one indicator will satisfy all criteria equally well. Ultimately, the choice of indicator is determined through a holistic assessment of validity and practicality. The selection

of indicators is an iterative process, building on consultations among managers, stakeholders, and partners. The process of selecting an indicator takes several steps, including brainstorming ideas, assessing each one, narrowing the list (using the SMART criteria), and finally, designing an indicator monitoring plan.

Once indicators are defined, management should identify targets that the program intends to deliver. This step can sometimes be arduous, because different people will have natural tendencies to prefer one target over another based on their personal priorities. The key is to prioritize the targets based on their degree of alignment with the business objectives. For example, if financial objectives carry the greatest weight within your organization, then attempt to set your most significant program target in this area. In this way, other valuable contributions of your program will not be as readily discounted but will be seen as enhancing the value of your program beyond making a threshold high-profile contribution.

(d) MEASURE INDICATORS. Once indicators are in place, management should establish mechanisms to collect the appropriate data and monitor performance. Be on guard for those who make numbers mean just about anything; management will be meticulous about whether the processes you use to collect and generate the program measures are valid. Management will be on the lookout to see whether you use reliable data sources, repeatable approaches, and consistent aggregation/calculation methods that will allow for year over year analysis.

(i) Quality Data—How Imperative Is It?. Naturally, people will want to say that data quality is paramount. However, the reality is that if you are using the same data sources that are used for measuring performance of the business objectives, then—even if the quality of the data in those sources is poor—it is still consistent and comparable (equally bad, so to speak). As a result, measures that pull from the same data sources already used by management to measure business performance will be less scrutinized than other data sources. Realistically, your program is going to have unique data sources, and that is where you should focus the bulk of your data quality assessment.

(ii) Repeatable Approaches. The significance of an indicator lies in the ability to report period over period to show directional performance. This cannot be achieved unless the approach for gathering the information for the indicator is repeatable. Repeatability is a factor of how often the data will be gathered. If you intend to report an indicator monthly, then the approach must be geared to collecting the same data at that same frequency. The time for collection needs to correlate to the routine upkeep of the source. If the information for the first report on an indicator was gathered on the 5th of the month from a system that is updated daily, then it is best to gather the information for the next month again on the 5th to capture a one-month period. Similarly, if the system storing the data is not updated for the prior month until the 10th of the month, then you must

realize that a lag in reporting exists in the source, and the indicator must reflect the same time period as the source.

(iii) Consistent Aggregation/Calculation. In a dynamic business environment, identifying aggregation and calculation methods that can be applied across an enterprise presents a significant challenge. So, calculation methods have to be normalized in the same manner or in a manner consistent with the way in which business performance measures are normalized.

(e) ANALYZE INDICATORS. You can gain tremendous insight into how to monitor indicators from the quality management discipline. Frameworks such as six sigma embody a powerful philosophy and set of tools that will help any organization improve its program. Some of the basic six sigma tools include:

- Descriptive statistics
- Histograms
- Pareto charts
- Line and run charts
- Scatter plots
- Control charts

Employing these tools can vary in sophistication. In essence, management should employ these and other techniques to understand whether program processes are operating within defined tolerances and meeting identified targets.

(f) IMPROVE AND CONTROL PROGRAM PROCESSES. To achieve program outcomes and deliver targets, an organization should design program processes and practices that are appropriately effective, efficient, and responsive.

(i) Effectiveness. As alluded to earlier, *effectiveness* describes the quality of a system along two dimensions:

1. *Design* effectiveness describes the degree to which a system or process is logically designed to meet legal and other defined requirements. Does the system or process contain all the necessary elements to thoroughly evaluate risk? Has it been designed for maximum effectiveness? If not, what features must be added to improve the system? Design effectiveness is very much a logical test that considers all requirements, risks, and boundaries and determines if the system is appropriately designed.
2. *Operating* effectiveness describes the degree to which a system or process operates as designed. If the system has been well designed, does it function correctly? Does it operate the way it was designed to? If not, how must it be managed to elevate its level of operation? Operating effectiveness helps management understand if, given a strong design, the system is operating as intended.

(ii) Efficiency. The concept of e*fficiency* captures the cost of the process or system—not simply the amount of money spent, but also the cost of human capital expended.

- *Financial* efficiency describes the total amount of financial capital required to execute a process.
- *Human capital* efficiency describes the type and level of individual(s) required to participate in the process. While human capital costs can be partially captured in purely financial terms, intangible opportunity costs must also be captured. In other words, if the program relies too heavily on senior executive time and focus, it may represent more than just purely financial costs (i.e., salary, benefits, and other overhead). An organization must also recognize the intangible costs of the loss of executive time and focus on other strategic objectives such as growth, profitability, talent retention, and customer loyalty.

(iii) Responsiveness. *Responsiveness* describes the system's ability to operate quickly and flexibly in response to changing circumstances.

- *Cycle time* describes the amount of total hours and/or total duration that it takes to execute a process. Cycle time is extremely important in a few program processes. For example, it is critical to minimize the lag time from when a problem occurs to the time it is detected. The program should also minimize the lag time from when an issue is detected to the time it takes to respond to the issue. For other processes, it is difficult to define clear lag time rules. For example, it is difficult to say how long it should take to investigate a particular issue, because each issue will have its own facts and circumstances.
- *Flexibility/adaptability* describes the degree to which the system can integrate changes, including new requirements (e.g., a new law, rule, or regulation) and/or new business units (due to merger and acquisition activity). These changes may be internal, as managers study the results of past performance evaluations and make needed alterations, or they may be external. New regulatory environments, changing market conditions, or altered public perceptions and concerns require the organization to make adjustments. A responsive system adapts quickly to changes in the environment. It also develops a long-range perspective, foresees more distant changes, and prepares for them.

Improvements then become part of the overall program where all of the standard management and control techniques should be used.

(g) PUTTING IT ALL TOGETHER. All of this can be daunting at first glance. The key is to use a logical, step-by-step approach. The profession is undergoing a

Program Outcome	Indicator Category	Indicator	Description
Culture: *Does the program inspire a principled culture of performance, accountability, trust, and open communication?*			
	Workforce Attributes	Ask individuals at all levels of the organization how these attributes are exhibited at all levels of the organization, including **executives, management,** and **staff.** It is important to understand not only how the individuals surveyed look at these levels, but also how they view their **direct supervisor** and their **peers.** All of the following indicators are based on employee perception surveys.	
		Emphasizes Integrity	% respondents who believe that [level] talks about ethics, integrity, and doing the right thing
		Demonstrates Integrity	% respondents who believe that [level] sets a good example for ethics, integrity, and doing the right thing
		Demonstrates Consistency (no hypocrisy)	% respondents who believe that [level]'s actions are consistent with the emphasis they place on the exercise of integrity by others
		Supports Integrity	% respondents who believe that [level] would support them to do the right thing even if it meant not making the numbers that quarter
		Keeps Promises	% respondents who believe that [level] keeps promises and commitments that they make
		Is Open for Discussion	% respondents who believe that they would feel comfortable approaching [level] to talk about issues related to ethics, integrity, and doing the right thing

EXHIBIT 68.5 INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Handles Pressure	% respondents who believe that [level] emphasizes integrity, demonstrates integrity, and keeps promises, even when under pressure to meet financial or other objectives
	Organizational Attributes	Ask individuals at all levels of the organization about the following organizational attributes.	
		Nonretaliatory	% respondents who believe that the organization does not and will not retaliate against individuals who report violations or misconduct
		Holds Everyone Accountable (at all levels)	% respondents who believe that [level] is held accountable when they violate policies
			% respondents who believe that [level] is held equally accountable to other levels in the organization when they violate policies
	Personal Attributes	Ask individuals about how they personally feel with regard to the organization, its direction, their role, and whether they feel prepared to fulfill their obligations. Some of these indicators are typically captured in an ''Employee Engagement'' survey conducted by human resources. This helps to provide context for other perceptions that an individual may have.	
		Understand Mission	% respondents who believe that they understand the organizational mission, vision, and direction
		Understand Position	% respondents who understand their job, where they fit within the organization, and how they contribute to its goals and objectives
		Feel Accountable	% respondents who feel accountable for performing their job and accountable for their actions

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Feel Pressured	% respondents who feel pressure to compromise ethics or integrity or to violate policies or the law (Note: It is also useful to capture the sources of pressure, including the level of the organization or other external pressures such as economic or family)
		Feel Frequent Pressure	% respondents who feel pressure frequently
		Feel Open to Discussion	% respondents who feel comfortable discussing ethics, integrity, and doing the right thing with people outside of the organization
		Satisfaction with Organization	% respondents who are satisfied with the organization
		Respect for the Organization	% respondents who respect the organization's mission, vision, and objectives
		Satisfaction with Job	% respondents who are satisfied with their job
Prevent: *Does the program actually prevent noncompliance and unethical conduct?*			
	Observed Misconduct	Ask individuals about observed misconduct and violations in the workplace over a specific time frame (e.g., over the past 12 months). Keep in mind that these indicators are perceptions and may not necessarily reflect fact (e.g., a person may observe something that they perceived is wrong or illegal, but it may, in fact, not be illegal). That said, the fact that someone perceives wrongdoing is in and of itself an important (even more important) indicator.	
		Observed Violation of Values	% respondents who believe that they observed violations of organizational or societal values, including unethical or aggressive behavior in the workplace

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Observed Violation of Policy	% respondents who believe that they observed violations of internal policies
		Observed Violation of Law	% respondents who believe that they observed violations of the law and illegal activity
		Perceived Types of Violations	Broken down by type, % of respondents who believe that they observed specific types of violations of values, policies, or law[1]
		Perceived Deterrence	% respondents who believe that misconduct will be detected and appropriately addressed
	Reported Misconduct	Look at the frequency and types of violations that were not prevented to understand how well the program is performing. A program will not be able to prevent all violations. However, over time, the program should get better and better at preventing, detecting, and responding to similar types of issues.	
		Reported Violations Rate	Number of reported violations per employee
		Frequency of Violation Types	Relative frequency of certain types of violations[2]
	Prevented Misconduct	While it is very difficult to prove a negative, the following indicators are good proxies for understanding if the program is preventing violations and noncompliance.	
		Willingness to Seek Advice	% respondents who feel comfortable calling a help line or seeking advice when they are not sure what actions to take
		Help Line Usage	Number of calls to the help line or similar mechanism per employee

[1]An organization should use a consistent taxonomy for misconduct, violations of policy, and illegal activity. The *OCEG Hotline/Helpline Handbook (HHH)* (www.oceg.org/view/HHG) is a free resource that provides a taxonomy for capturing issues that may be a useful thought starter.
[2]Ibid.

Exhibit 68.5 (*continued*) Indicators for Measuring Performance

Program Outcome	Indicator Category	Indicator	Description
		Proactive Detection of Weakness	Number of weaknesses in the program detected during an ongoing or periodic effectiveness evaluation
Prepare: *Does the program actually prepare the organization to address key risks, non-compliance, and unethical conduct?*			
	Perceived Skills	It is important for the workforce to have the right skills to understand what compliance and ethics issues present operational risks and how to deal with them up to and including reporting them, if appropriate. One way to understand this is to ask individuals about their perceived level of skill.	
		Perceived Recognition of Risks	% respondents who believe that they have the skills to recognize ethical and compliance challenges
		Perceived High-Risk Jobs	% respondents who believe that their job presents a high level of compliance and ethics operational risk to the organization and they are not adequately prepared to handle it
		High-Risk Job Preparation	% of high-risk job respondents who feel prepared to handle the compliance and ethical operational risks they face
		Perceived Ability to Ask Questions	% respondents who believe that they know how to seek advice if they have a question
		Perceived Ability to Report Violations	% respondents who believe that they know how to report a violation of values, policies, or law
	Evaluated Skills	Another way to understand this is to use skills assessment and performance appraisals to understand whether the skills exist.	

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Appraised Integrity	% employees who are evaluated as satisfactorily exhibiting integrity
		Appraised Skills	% employees who are evaluated as satisfactorily exhibiting skills to address ethical and compliance challenges that they face in their job
		Assessed Skills	% employees who pass a skills-based test in appropriate risk areas given their job
	Practiced Skills	For high-risk areas, some organizations practice responding to events to ensure that they are fully prepared for when they occur.	
		Critical Risks Preparation	% critical risks that have gone through preparation exercise (e.g., simulation, tabletop exercise, etc.)
	Information Management	Perceived Ability to Respond to Information Requests	% respondents who believe that information is appropriately created, stored, and managed so that, if required, an accurate record of history and fact can be produced
Protect: *Does the program adequately protect the organization from negative consequences if/when noncompliance and unethical conduct materialize?*			
	Coverage	A critical aspect of every program is to provide adequate coverage of risks, including legal and regulatory risks. These are typically part of an effectiveness evaluation.	
		Critical Risk Coverage Breadth	% of critical risks that have control and accountability in place

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Critical Requirement Coverage	% of critical requirements that are addressed (e.g., federal sentencing requirements, specific legal or regulatory requirements) by some form of control
		Critical Risk Coverage Depth	% of critical risks that have multiple layers of control in place (e.g., not just a policy, but also training, preventive controls, detective controls, and workforce controls such as compensation and performance appraisal incentives, etc.)
		Critical Risk Coverage Assurance	% of critical risks that have assurance from an objective party (internal or external) that controls are designed and operating appropriately
		Supply Chain Coverage	% of key suppliers that have contractual commitments aligned to risk tolerance (e.g., if you have significant compliance or ethics operational risk with one of your suppliers, you may include supplier audit provisions, indemnification, and limits in your contracts with that supplier)
	Insurance	An important and often overlooked part of a program is adequate insurance coverage for high-risk areas.	
		Insurance Coverage	% key risk areas that have level of insurance coverage consistent with risk tolerance mandates of the organization

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
Detect: *Does the program actually detect noncompliance and unethical behavior when they occur?*			
	Workforce Perceptions	Perceived Detection	% respondents who believe that violations and misconduct are actually detected
		Propensity to Report Violations	% respondents who observed violations and actually reported the violations
		Reasons for Not Reporting	Capture the reason that people did not report, including: • Issue was resolved • Did not think it was significant • Did not want to get someone fired • Did not think it was my responsibility • Fear of retaliation • Did not think anything would be done • Did not know who to contact • Did not believe it could be reported anonymously • Believed the individual self-reported • Knew someone else had reported • Believed someone else had reported
		Retaliation	% respondents who reported a violation and believe that they experienced retaliation
	Process Indicators	Detection Lag Time	Number of days it took for the organization to actually detect a violation (time/day of actual incident or incidents to the time/day when it was first detected)

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Reasons for Detection Lag	Capture the key reasons for lag in detection
		Reported Lag Time	Number of days it took for the incident to be reported
		Reasons for Reporting Lag	Capture the key reasons for lag in reporting
		Reactive Detection Rate	Number of weaknesses discovered after a violation actually occurred
		Non Detection Rate	Number of weaknesses discovered by authorities or other external source before the organization was able to discover it
Respond: *Does the program appropriately and quickly respond to events once they are detected?*			
	Workforce Perceptions	Perceived Speed of Response	% respondents who reported a violation who are satisfied with the speed of response
		Perceived Quality of Response	% respondents who reported a violation who are satisfied with the quality of the response (i.e., they are satisfied with the outcome)
	Process Indicators	Response Lag Time	Number of days it takes to respond to a reported violation (time/day of reported incident to the time/day an initial response was made)
		Cause of Response Lag	Capture the root cause of any lag in response
		Issue Resolution Cycle Time	Number of days it takes to resolve an issue once it is detected (while every issue will have its own set of circumstances and facts, similar issues should be compared so that the organization gets better and better at handling similar issues)

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
Improve: *Once the organization detects and responds to a weakness, is the weakness actually fixed so that similar events do not materialize in the future?*			
		Repeat Issues	% substantiated violations that are similar to previous violations
Reduce Loss: *Does the program reduce the tangible and intangible damage caused by noncompliance and unethical behavior?*			
	Tangible Noncompliance Loss	Losses associated with noncompliance and other violations can mount. Ideally, an organization should track direct costs associated with the investigation and ultimate resolution of an issue to better understand how much the organization lost because of the event/issue.	
		Internal Investigation Cost	$ spent on internal resources to investigate issues
		External Investigations Costs	$ spent on external staff and experts to investigate issues
		Fines and Penalties	$ extracted from the organization in fines, penalties, and judgments
		Impairment of Assets	$ impairment of assets as a result of noncompliance or other violations
		Market Cap Reduction	$ in market capitalization that is judged to be related to noncompliance or other violations
		Workforce Turnover	Number of staff who voluntarily left and cited compliance and ethics issues as a reason for leaving
		Business Interruption	$ value of business that was interrupted because of noncompliance or other violations
	Intangible Noncompliance Loss	Some losses can be difficult to quantify. However, there are some effective means to better understand the impact that noncompliance and other violations have on these important areas of the business.	
		Reputational Loss	% change in customer or supplier confidence in organization caused by noncompliance or other violation

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Negative Media	% change in negative media caused by noncompliance or other violation
Optimize Costs: *Does the organization continuously optimize costs to deliver similar or even improved outcomes?*			
	Direct Costs	Direct costs include fully loaded staff costs and expenditures on technology and other assets that are part of the program.	
		Planning Costs	$ spent on people and technology to set objectives, identify and assess risks, and put a plan in place
		Preventive Costs	$ spent on people and technology to develop a code of conduct, policies, procedures, and other controls; develop and deliver training; design and implement workforce incentives and other controls; and execute preparation exercises intended to prevent issues
		Insurance Costs	$ spent on insurance premiums
		Monitoring & Detection Costs	$ spent on people and technology including the hotline/help line and other monitoring and auditing activities intended to detect issues
		Response Costs	$ spent on people and technology to respond to issues, including investigations
		Improvement Costs	$ spent on people and technology to improve the program after issues are discovered
Enhance Stakeholder Perception of Value: *Does the program improve stakeholder perceptions of the organization?*			
	Governance Ratings	There are a number of governance ratings agencies, and most of them factor legal and regulatory risk management into their equation.	

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

Program Outcome	Indicator Category	Indicator	Description
		Governance Metrics	% change in GMI rating
		Institutional Shareholder Services	% change in ISS rating
		Audit Integrity	% change in Audit Integrity rating
		Corporate Library	% change in Corporate Library rating
	Credit Ratings	Credit ratings agencies have started to look at the way an organization conducts risk assessment as input to ratings (e.g., in the financial services industry). There is a strong suggestion that this trend has already worked its way into other industries.	
		Standard & Poor's	% change in S&P rating
		Moody's	% change in Moody's rating
	Media Coverage	Media serves as a proxy for and help to drive public opinion. Favorable vs. unfavorable media can affect the perceptions of customers, suppliers, partners, employees, and regulators.	
		Change in Media Coverage	% change in favorable vs. unfavorable media coverage
	Other Stakeholders	Customers are more willing to provide repeat business to and be less price sensitive with organizations they respect.	
		Suppliers are will to extend more favorable credit terms, guarantees of quantities, and so on to organizations that they believe act more responsibly.	
		Labor organizations strike better deals with, operate more openly and directly with, refrain from litigation with, seek fewer concessions from, and strike more infrequently against reputable organizations.	
		Regulators and government officials will more often adopt or agree with regulatory proposals presented by organizations they can trust to do the right thing.	
		Satisfaction/Opinion	Track satisfaction and opinion metrics from all of these stakeholder groups

EXHIBIT 68.5 (*continued*) INDICATORS FOR MEASURING PERFORMANCE

tremendous shift from focusing on just legal requirements and program features to a more holistic approach focused on business performance. Those who establish strong and structured risk assessments in the first place, and then verify the design and operation of their program and approach, will surely realize both organizational and personal benefits.

(h) CANDIDATE INDICATORS[7]. Exhibit 68.5 may help you define indicators to measure the performance of your program. It would be cumbersome for most executives to measure and monitor each of these indicators. A general guideline is to use no more than 15 indicators to manage a process. That said, executives who seek to develop a robust metrics program may consider delegating some of these metrics to members of their team, so that a total picture can be developed over time.

Notes

1. This chapter is drawn from articles previously published by Mr. Mitchell and Ms. Switzer, and some portions were originally published in the *OCEG Program Metrics and Measurement Guide (MMG)*, which is available for free download at www.oceg.org/view/MMG. © 2007, OCEG. All rights reserved.
2. The term *stakeholder* will be used broadly from this point to distinguish all impacted parties, including employees, customers, vendors, trading partners, and so on, from lawmakers, law enforcement, and regulators.
3. For an example of training, look at California's AB 1825, which has specific provisions for how harassment prevention training should be designed and delivered. Employees are required to take one hour of harassment prevention training every other year. The duration is mandated. There is no outcome measurement required.
4. Quality management and six sigma practitioners should notice that this approach is strongly related to and is meant to work with a define, measure, analyze, improve, control (DMAIC) cycle. This approach takes define and splits it into three steps starting with strategic objectives and ending with specific indicators.
5. In this context, "compliance" is used broadly to encompass compliance with laws, rules, and regulations (mandated boundary) as well as internal policies and voluntary commitments (voluntary boundary).
6. These indicators were originally published in an OCEG webinar called "Making the Business Case for Integrated Governance, Risk, and Compliance," an archive of which is available for free download at www.oceg.org/webinars.aspx. © 2007, OCEG. All rights reserved.
7. These indicators were originally published in the *OCEG Program Metrics and Measurement Guide (MMG)*, which is available for free download at www.oceg.org/view/MMG. © 2007, OCEG. All rights reserved.

CHAPTER 69

ACCOUNTING, BUDGETING, AND REPORTING—HOW IS THE REGULATORY FRAMEWORK CHANGING IN THE PUBLIC SECTOR?

Massimiliano Claps

69.1 INTRODUCTION: ACCRUAL AND CASH BASED—WHAT DOES IT MEAN?

Two main accounting bases exist for recognition and measurement: the accrual basis and the cash basis.

1. Accrual-based accounting recognizes income in the accounting period in which it is earned, regardless of when the cash is received. Expenses are recorded when they are owed, instead of when they are paid.
2. Cash-based accounting recognizes receipts when cash is received and deposited and payments when bills are paid within the accounting period.

According to the International Federation of Accountants, this has implications for the type of statements that are presented. When the accrual basis of accounting underlies the preparation of the financial statements, the financial

statements will include the statement of financial position, the statement of financial performance, the cash flow statement, and the statement of changes in net assets/equity. When the cash basis of accounting underlies the preparation of the financial statements, the primary financial statement is the statement of cash receipts and payments.

69.2 PUBLIC SECTOR MIGRATION TO ACCRUAL ACCOUNTING: PROS AND CONS

Government financial accounting has traditionally consisted of providing an outturn report, comparing the actual payments and receipts with those which were authorized in the budget by parliament. In essence, traditionally governments have used a cash basis for accounting for their finances. In most cases this was a modified cash-based accounting system, as some specific solutions had to be adopted, such as expenses are accounted for as they are paid, with accounts being kept open at the end of the year to account for expenses that relate to that year.

This approach still forms the basis for the practice of several governments across the world. It is a simple approach, which provides assurance through the audit of such accounts that government spending has been in line with the agreed budget and that fraud and other irregularities have been minimized. Cash-based accounting has the virtues of simplicity and objectivity. However, the cash basis has significant weaknesses: There is no matching requirement, information about assets and liabilities is frequently very limited, and there is the lack of an effective balance sheet.

Accrual-based accounting has the potential to produce more transparent and meaningful financial information. Thus over the past ten years an increasing number of governments at all levels have started to move to an accrual basis of accounting and budgeting. The benefits of accrual accounting include:

- Accrual-based International Public Sector Accounting Standards are more complete than cash-based accounts, and by definition they also remove the scope for the manipulation of payments and receipts in order to suit reporting and control objectives (although leaving scope for other forms of manipulation).
- The information available from accrual-based accounts facilitates a better quality of management and decision making, including over the allocation of resources.
- There is an opportunity to change organizational behavior through the use of incentives and penalties, including comparisons with the costs of the provision of services by the private and voluntary sectors.
- There is an opportunity to establish effective performance measures that are not impacted by the vagaries of the timing of cash payments and receipts and that include information about fixed and current assets and liabilities.

- The costs of capital assets are spread over the useful lives of these assets.
- There is a more effective and reliable assessment of the financial health of the organization, through a correct and complete recording of all debts and amounts receivable.
- In addition, financial indicators on an accrual basis are helpful in assessing the influence of fiscal policy on aggregate economic demand.

Despite its advantages, accrual accounting also has some shortcomings that international experts and national regulators are trying to deal with.

- The accrual basis is a much more complex system than the traditional cash system. It requires a higher degree of judgment than the straightforward cash basis, particularly over valuations of physical assets and provisions. This means governments will have to hire and/or train the expert resources capable of understanding the complexities of the system and also able to manage and maintain the more sophisticated accounting infrastructure. An auditor who is trained to audit accrual-based financial reports will also be a requirement.
- Goods and services in the public sector differ from those in the private sector. In the private sector, goods and services are generally rival and excludable, which makes it possible to practice full accrual accounting: Receipts are recognized according to merchandise sale and service delivery, and matched with related expenses. Since goods and services delivered by the government are public (i.e., nonexcludable and nonrival), the government is unable to charge for individual use of public goods and services and thus is unable to avoid free-rider problems. Instead, the government has to resort to imposing payments (i.e., taxes) on both users and nonusers alike to finance the public goods, meaning that the government delivers public goods and services to both taxpayers and nontaxpayers. This situation creates a disconnect between taxes and delivery of services in the short term and at the individual level, and many transactions are nonreciprocal. Therefore, it is unrealistic to use the same full accrual basis (as in business accounting) in government accounting. No government has linked the recognition of its general revenue to service delivery.
- The public sector contains agencies to deliver public services as well as enterprises and organizations funded by government. Those publicly owned corporations (or government business enterprises), for example operating in postal services, utilities, and transport, offer services that differ from pure-public goods and rather mimic private goods and services. Therefore government business enterprises are required to comply with International Accounting Standards (IASs) issued by the International Accounting Standards Committee.
- Governments own a series of very specific assets that are difficult to put in a specific category and to evaluate. For example, how should historical

palaces be valued when being used as government offices? Should they be treated as general assets and depreciated like ordinary office buildings, or be treated as valuable heritages? Or how should military research be capitalized, since military costs may be difficult to track due to subjective accounting decisions on how to separate commercial value from military purpose?

- The valuation of assets specific to the public sector is also controversial. Usually, there are two valuation approaches: One uses historic cost; the other uses a current cost approach, including depreciated replacement cost, value in use, and net realizable value. Different valuation methods could be used according to the situation in the private sector; however, the valuation issue is more complicated in the public sector. The historic approach provides an easy way to value and record, because the value can be tracked from the acquisition cost and subsequent depreciation. But even this could create a problem of unrealistic value information and deviation from the current value of the assets, meaning that authorities would be unable to evaluate the performance of an entity correctly. Current valuations are believed to reflect more relevant cost information and better information about performance. The current approaches require many professional judgments to be made, because the depreciated replacement cost, value in use, or net realizable value of the assets in the public sector usually are difficult to determine.
- On the liabilities side, the government assumes limitless obligations pertaining to a number of social issues (e.g., pollution and social security), risks, and contingent liabilities. Related questions arise: If noncontractual exchange transactions such as social insurance programs are treated as a liability, then should other important long-term commitments such as expenditures for education and public health be treated as liabilities?

To facilitate the adoption of accrual accounting and overcome some of these pitfalls, governments have generally adopted accounting standards, either in the form specified by the International Public Sector Accounting Standards Board (IPSASB) of the International Federation of Accountants (IFAC) or by adapting private sector accounting standards.

69.3 INTERNATIONAL PUBLIC SECTOR ACCOUNTING STANDARDS

The IPSASB has set itself the task of developing a full set of international public sector accounting standards and ensuring that these are adopted as widely as possible:

- It issued 21 accrual-basis standards and one comprehensive cash-basis International Public Sector Accounting Standard (IPSAS) (latest update available on 2006 IFAC Handbook of International Public Sector Accounting Standards Board Pronouncements), thus establishing a core set of

financial reporting standards for public sector entities. The IPSAS 1 standard for public sector accounting states: "Accrual basis means a basis of accounting under which transactions and other events are recognized when they occur (and not only when cash or its equivalent is received or paid). Therefore, the transactions and events are recorded in the accounting records and recognized in the financial statements of the periods to which they relate. The elements recognized under accrual accounting are assets, liabilities, net assets/equity, revenue and expenses."

- The IPSASB published a transition guide: Study 14, Transition to the Accrual Basis of Accounting: Guidance for Governments and Government Entities.
- The board is working on a second phase of its standards-setting program, which includes the development of guidance on key public-sector-specific issues not fully dealt with by the existing IPSASs. Examples of topics are impairment of cash-generating assets, development assistance, public-private partnerships, and heritage assets.

69.4 ADOPTION OF ACCRUAL ACCOUNTING IN EUROPE

European countries have additional reasons to adopt a common set of accounting standards, first of all the existence and continuous extension of the European Union. It is critically important that some level of harmonization is reached throughout the European Union members to monitor the application of the Maastricht Treaty, which requires harmonization of monetary and fiscal policies of member states adopting a common currency. Despite the existence of the European System of Economic Accounts—Council Regulation (EC) No. 2223/96 of June 25, 1996, and related regulation for national and regional accounts, frequent debates on the figures provided by member states and used by the European Commission to enforce the Stability and Growth Pact and to enhance coordination of public finance policies require improved and comparable statistics on public finances.

The European Union is certainly a key driver pushing toward harmonization of government accounts; however, the need to produce and analyze more comprehensive accounting data became pressing at the national level in the 1990s. Finance ministries had lost control of spending growth, while the European Union was imposing stricter limits, such as a deficit-to-gross domestic product (GDP) ratio below 3 percent, in preparation for the introduction of the euro. Challenged by the need to impose more thorough surveillance on public sector governance, national governments introduced new regulations or launched modernization plans to inject businesslike practices in order to improve efficiency, transparency, and accountability; accrual accounting and budgeting and cost accounting were among the key areas of intervention to help decision makers move to a management based on outputs and not preauthorized inputs.

	1970s–1980s	1990s	After 2000
Local government	Switzerland, the Netherlands, Sweden	Spain, France, Finland, UK	Germany, Italy
Central government		Spain, Finland, Sweden, UK	Switzerland, France

Source: European Commission and FEE data, 2004.

EXHIBIT 69.1 DATE OF START OF ACCRUAL ACCOUNTING REFORM

Currently various forms of accrual accounting exist in Sweden, Portugal, Denmark, Switzerland, France, Germany, Italy, and the UK. Spain, the UK, Sweden, and Finland have largely completed their move; France is expected to complete its plan in 2006. Local authorities in Italy and Germany are advancing even when the national authorities remain undecided (see Exhibit 69.1 and also appendix).

In terms of standards, IPSASs are currently adopted (entirely or partially) in France, Netherlands, Norway, and the UK.

The European Commission itself launched a multi-annual plan in 2000 for the modernization of its accounting framework, which comprised:

- Undertaking a study on the establishment and presentation of the accounts of the EU delivered in mid-2000 by high-level experts on public accounting.
- Drawing up in June 2001 an action plan for modernization, which was discussed with the Court of Auditors. The Court has welcomed the document orientations.
- Proposing in 2001 accrual accounting as obligation in the new Financial Regulation, which was adopted by the legal authority in 2002.
- Introducing elements of accrual accounting in the presentation of the financial statements.
- Calculating the economic out-turn since 2000.
- Adopting an accounting and consolidation manual for all the Institutions.
- Analyzing several member states' experience (United Kingdom, France, Sweden, Spain, Netherlands).
- Adopting on December 17, 2002, a detailed action plan for the introduction of accrual accounting by 2005 (see IP/02/1904).

(a) FRANCE. France has broken with the tradition of expenditure-oriented budgets by drawing up a framework for budgeting and accounting based on a three-tier structure. The missions correspond to the state's major public policies. Each mission comprises a set of programs to which appropriations are allocated and broken down into subprograms (actions) that together constitute the operational means of implementing the program. The previous budgetary structure

(dated 1959) based on budget chapters obscured the ultimate aims of budget appropriations and the cost of administrative policies and structures.

This transformation began in 2001 with the reform of state budgeting and accounting, through the approval of a new regulation (LOI organique no 2001-692 du 1er août 2001 relative aux Lois de Finances-LOLF). The Minister for Budget and Budgetary Reform (Ministre Delegue au Budget et à la Reforme Budgetaire), part of the Ministry of Finance, Economy and Industry (MINEFI), has been in charge of coordinating this modernization. This bylaw has been designed to make public spending more transparent and to improve performance measurement across all levels of public administration. LOLF introduced new rules for preparing and implementing the state budget; the aim of the new rules is to move from a resource-based to a results-based approach. Henceforth, debate should concentrate on the objectives and the cost-effectiveness of public policies. Previously, the preparation and examination of the budget bill focused primarily on quantitative variations in appropriation amounts, without systematically linking these variations to expected results and actual outturn. The shift of focus to performance presupposes that performance can be measured objectively. That is what Article 51 of the LOLF assumes when it states that state actions are presented having regard to "related costs, objectives pursued, actual results, and results expected in the years to come, measured using precise indicators whose choice is substantiated." Chapter V of the new law, which entered into full force with the preparation of the 2006 budget, states that:

- The state must prepare a revenues and expenses budget; maintain general accounts of operations; and implement management accounting practices to analyze the cost of its operations (art. 27).
- The budgetary accountancy is cash-based (art. 28).
- The general accounts of operations are accrual-based (Art. 30).

As part of this reform, France has dedicated significant effort to simplification, for instance by reducing its 1,850 budgetary chapters to 300 policy areas/missions and also by integrating the supporting IT solutions. Within the cadre of modernization of government back-office functions, the Accord project was launched aiming to consolidate expenditure management and accounting systems across the entire central government, but the project went through a rather bumpy road:

- In 1999, Accenture and PeopleSoft were awarded a contract to deploy a financial accounting system for central agencies of the state.
- In 2001, with the approval of LOLF, an Accord 2 project—with the challenging objective of extending standard accounting software applications to all local offices of the central government—was automatically launched to modify the first application, while the Accord 1 implementation was still ongoing. The new legislation was planned to enter into force in January

2005—thus the platform needed to be operational from January 2006 to support the financial accounting of 2006 budget provisions.

- Between 2002 and 2003 the second phase of the Accord was broken down into two projects:
  1. Accord 1bis, which entailed the extension of the first platform to 30,000 users (approximately five times more than the original project). The contract was awarded to the existing providers. Completion was expected for 2004.
  2. Accord 2, which aimed to integrate all users across central ministry's offices and their local branches. A €200 million call for tender was issued to start the project in 2004.
- In 2004 SAP, Accenture, and Capgemini won the new contract. But in May the then Minister of Finance, Nicolas Sarkozy canceled the contract because of complaints raised by competing consortiums.
- During 2005 the Accord project was progressively restructured. The Agency for State Finance IT (Agence pour l'informatique financière de l'Etat—AIFE) was put in charge of achieving the same goals. The MINEFI replaced the Accord program with two new projects: the Palier 2006 project will aim to adjust Accord 1bis at the central level to comply with short-term LOLF obligations, while for the long term the Chorus project is to be launched with pilots in 2007 and full deployment to be started in 2008.
- In summer 2005 AIFE indicated that the Palier 2006 project should aim to adjust Accord 1bis at the central level to comply with short-term LOLF obligations, while for the long term the Chorus project was to be launched with pilots to be done in 2007 and full deployment to be started in 2008.
- At the end of March 2006, the French government selected SAP for public sector solutions to enable its Chorus project. The government opted for a single SAP platform, replacing all existing applications, including Oracle/PeopleSoft software, across all central ministries and their regional services. Following consideration of solutions presented by SAP and competitors, including Oracle, the French government selected SAP applications to support the administration's Chorus program. The deployment of SAP for public sector solutions on the SAP NetWeaver platform is expected to serve up to 25,000 users by 2009 and to create a new three-dimensional accounting system covering budgeting, fiscal year accounting, and cost analysis.

At the local government level, the National Code of Local Administrations (Code Général des Collectivités Territoriales—CGCT), first published in 1996 and refined in the following years (e.g., Arrete, 1997-12-04, Relatif a l'Instruction Budgetaire et Comptable M 14 des Communes et de Leurs Etablissements Publics Administratifs), defines all the details of budgetary and financial accounting for

local governments. Municipalities are, for instance, required to prepare two budgetary accounts (the accounts of consumption of budgetary provisions and the account of realized revenues and expenses) and to maintain financial accounts of assets and liabilities on an accrual basis. The new French plan for government IT investments (ADeLE) highlights two key Enterprise Resource Planning (ERP) initiatives for local administrations, Helios 1 and Helios 2. The first phase will entail the deployment of applications for budgeting, expenses and revenue accounting, debt management, inventory and purchasing; the second phase will encompass financial, treasury, reporting, and cost accounting.

(b) GERMANY. Traditional governmental accounting in Germany is input oriented, cash based, compliance oriented, and primarily aimed to meet the budgetary control needs of the legislature. German governmental budgeting and accounting at all three levels of government (federal, Länder, and local) are regulated by law and not by any government-external standard-setting body.

The legal framework of governmental accounting is a hierarchy comprising:

- Chapter X (Finance) of the Basic Law
- The Budgetary Principles Act of 1969 (Haushaltsgrundsaetzegesetz), which is a piece of "framework legislation" enacted according to Article 109, Para. 3 of the Basic Law: "Through federal legislation . . . principles applicable to both the federation and the Länder may be established governing budgetary law, budget management, and multiyear financial planning"
- The Federal and State Budgetary Acts of 1969–1971 (Bundeshaushaltsordnung und Landeshaushaltsordnungen)
- The Municipal Budgetary Acts of 1972–1974 (Gemeindehaushaltsverordnungen)
- Federal and state regulations specifying the stipulations of the Budgetary Acts (Verwaltungsvorschriften zur Bundeshaushaltsordnung und den Landeshaushaltsordnungen)

The accounts of the core governments (federal, state, and local entities excluding public corporations, universities, social insurance funds, etc.) are kept on a modified cash basis. All revenues and expenditures are recorded twice, when due and when collected or paid, respectively. The amount of revenues and expenditures due but not received and collected at the end of the fiscal year (which is the calendar year) are shown in the accounts as receivables and payables. The bookkeeping method used is single entry called Kameralistik accounting. Article 114 Basic Law requires the minister of finance to "submit to the Bundestag and the Bundesrat annual accounts for the preceding financial year covering all revenue and expenditure as well as assets and debts." The main component of the annual accounts is the line-by-line statement of actual revenues and expenditures whereas the statement of assets and liabilities is only an incomplete annex containing just monetary assets and capital market debt.

The objective of the 1997 amendment to the Budgetary Principles Act (Budget Law Development Act of 22 December 1997) was to provide governments with more flexibility in budget management and thus strengthen cost-consciousness in using scarce financial resources. This was expected to be achieved by extending the possibility of transferring funds between budget lines and of carrying forward unused appropriations as well as by opening an option for introducing cost accounting in government "where appropriate." Moreover, the Bundesrat succeeded in adding two new sections to the Budgetary Principles Act. According to section 6a, global budgeting of governmental entities on a cash basis is allowed on the condition that:

- Appropriate information and control devices are available to ensure keeping the actual net expenditures within the budget limits.
- Outputs are specified and included in the budget or another legal document.
- Appropriations are also shown in the traditional way (i.e., by object of expenditure).

In addition, Section 33a now permits a government to shift its financial accounting system to an accruals base but again without abandoning the former cash-based system.

The stance of the federal government, particularly the minister of finance so far has been that neither output-oriented and accrual-based budgeting nor accrual financial accounting are necessary and beneficial for sound governmental financial management. Increased budget flexibility and the introduction of cost accounting in appropriate governmental entities are considered sufficient to remedy the weaknesses of traditional budgeting and governmental accounting. The present situation in the federal government can be described as a patchwork of cost accounting systems of varying degrees of sophistication, at different stages of development with different significance as a management tool. These systems are stand-alone systems (i.e., they are not linked to the budget and the budgeting process).

Most of the Länder governments prefer an approach similar to that of the federal government. This means that the existing cash-based budget is enhanced by output information, and the cash-based financial accounting is supplemented with cost and performance information for either all or just selected core government entities. An exception is the government of Hessen, which decided in 1998 to convert its traditional input- and cash-based budgeting and accounting system to an output- and accrual-based system for all governmental entities and the whole of government over a ten-year period. Even though the parliamentary majority and thus the government changed in 1999, the reform approach and its time horizon remained unchanged. Now, with a time lag of several years, other Länder have either decided to add to the traditional cash accounting system an accrual-based financial accounting system and submit a balance sheet and an operating statement (Bremen, Hamburg) or expressed the intention to do so

(Northrhine-Westphalia). But there still is a legal obstacle for more fundamental reforms such as the Hessian case: the Budgetary Principles Act as of today does not allow Länder governments to completely abandon traditional budgeting and accounting.

Local governments started much earlier discussing the pros and cons of an accounting reform toward accrual and experimenting with accrual-based systems than federal and Länder governments did. Thus, there was a need for the Länder ministries of the interior, responsible for local government budgeting and accounting law, to think about necessary legal amendments. A first step toward reforming the accounting system was the amendment of the Municipal Acts and the Municipal Budgetary Acts in the 1990s by "experimentation clauses." This amendment permitted local governments to apply budgeting and accounting approaches other than the ones provided for by legislation for a limited period of time. Furthermore, the Standing Conference of the Länder's Interior Ministers established a subcommittee "on municipal budget law" charged with specifying the legal provisions for an output- and accrual-based local government budgeting and accounting system to be included in the Municipal Budgetary Acts. The subcommittee submitted amendment guidelines for an output and accrual-based budgeting and accounting system as well as for an updated kameralistik accounting system in summer 2003. The Standing Conference passed these guidelines in November 2003 and it is now up to the Länder to amend its local government budgeting and accounting law accordingly. In doing this, the individual Länder can make the new output- and accrual-based system an obligatory requirement or just an option for the municipalities. Northrhine-Westphalia and Lower Saxony intend to shift their budgeting and accounting systems over a multiyear transition period to an accruals base.

In parallel with the regulatory reform, pilot projects—aimed at developing a conceptual basis for governmental accrual accounting and accruals and output based budgeting, initiating the necessary software developments, gaining experience with the new approach and possibly modifying it, and not least providing an impetus for amending local government accounting law—were set up in selected cities and counties of several Länder, particularly Baden-Wuerttemberg, Hessen, Northrhine-Westfalia, and Lower Saxony. The city of Wiesloch (Baden-Wuerttemberg) was the first one to run such a pilot project, followed by Hessian (1998), Northrhine-Westfalian (1999), and Lower Saxon local governments (2001). The Wiesloch project commenced in 1994 and was by and large completed by June 30, 1997; the city government partnered with the Ministry of the Interior, the German Postgraduate School of Administrative Sciences in Speyer, the Regional Computer Center in Heidelberg, and software vendor SAP. Most of those pilot projects are now completed, and the new systems are in regular operation in the pilot cities and counties.

The Institute of Public Auditors in Germany issued an exposure draft of an accounting standard for the public sector in December 2002. The proposed

accounting principles were based on the requirements of the German Commercial Code. Members of the Institute of Deutsche Wirtschaftsprufer Public Sector Committee held several meetings with representatives of different states to discuss the exposure draft and to stress the importance of developing a harmonized set of accounting standards.

(c) ITALY. The process of reform of Italian public sector accounting started in the early 1990s as a consequence of reforming of administrative processes (Legge 241/90 Norme in Materia di Procedimento Amministrativo e di Diritto di Accesso ai Documenti Amministrativi); in fact, the first article of this law states that public administration activities are governed by principles of efficiency, effectiveness, and transparency. From the mid-1990s, accounting of local health units has been accrual-based (also budget); since the late 1990s accounting of local authorities (communes and provinces) has been characterized by a twofold approach: modified cash- and accrual-based carried out at the same time (but only cash for budget).

Central administrations, regions, and a large number of other public sector bodies (e.g., social security funds) still use traditional modified cash-based accounting, even if cost and management accounting is compulsory for all public administrations since 1997 (Dlgs. 7 agosto 1997, n° 279). Accounting and budgeting at the central government level are still based on cash-based criteria and regulated by Royal Decrees issued in 1923 and 1924 and modified by laws 62/1964, 468/1978, 362/1988, 94/1997, and 208/1999.

The key requirements concerning central government accounting were passed in 1997 under Law 94 and under Legislative Decree 279, which governs its enforcement. The annual budget includes a document of total government revenues and another document of total government spending broken down by ministry. The budgets of autonomous enterprises and agencies are also enclosed. Each document of government spending is accompanied and illustrated by preliminary notes and is supplemented with a technical annex. The national annual budget is still drawn up both on an accrual basis and on a cash basis. Parliament ratifies by law both accrual-based and cash-based estimates. The budget performs an authorizing function inasmuch as spending estimates establish the limits (i.e., spending caps) within which it is possible to enter into obligations and to make payments, respectively. The most significant innovation introduced under Law 94 concerns the elements of revenue and spending through the introduction of basic budgeting units that are to be approved by Parliament:

- Revenues are subdivided into headings (source), basic budgeting units, classes (nature of assets), and items (for bookkeeping purposes only).
- Spending is subdivided into goal functions (public policies), basic budgeting units and items (for bookkeeping purposes).

At the local government level, a 1995 reform was passed by the national parliament, to make financial management consistent with the recognition of greater autonomy for local government enacted with 1993 reform of the electoral system, which allocated more powers to mayors and changed profoundly the form of local government accountability. The Law 421/1992 paved the way for the reform of local government accounting. The Ministry of the Interior in 1993 set up an ad hoc committee comprising representatives from different professional fields, mainly the chief financial officers of local governments, and charged them with the task of drawing up a reform proposal. The 1995 reform kept budgetary accounting as the pivot of the entire local government accounting system. Estimated spending in the budget should be "paid for" by revenues of the same amount. Any budgetary deficits should be eliminated in the ensuing fiscal year by increasing revenues or by cutting spending. Besides budgets, the Local Government Accounting Act requires local governments to produce an annual statement of operations and a statement of assets and liabilities in a standard format established under Law 194/1996. Double-entry bookkeeping, however, is not mandatory. Alternatively, local governments can still use the traditional single-entry obligation- and cash-based accounting system and produce accrual-based financial statements through a system of year-end adjusting entries. A reconciliation statement must be included in the financial statement to reconcile the cash- and obligation-based statement with the income statement. Notwithstanding the reform, limited progresses have been made in terms of quality of economic information or quality of decisions taken by local governments.

The current situation is highly fragmented and somewhat confusing, generating serious lack of mutual understanding of data and in turn potentially harmful consequences in policy-making terms, such as in the case of health care provision where local health authorities (AUSLs) have fully adopted accrual-based accounting, while their controlling and financing entities (regional governments) continue using cash-based methods.

Over the past several years various initiatives were undertaken to encourage harmonization.

- The Consolidated Act of Local Authorities in 2000 followed by the creation of an Observatory on Accounting and Finance of these bodies within the Ministry of Interiors with the task of producing and promoting accounting standards for communes and provinces (to be endorsed by the Ministry). To date, three are the accounting standards issued as well as a framework, which follows the IASB's Conceptual Framework with some variations due to the peculiarities of the public sector; the standards refer to (1) planning and programming, (2) operations management, and (3) reporting.
- The Presidential Decree no. 97/2003, regulating noneconomic public bodies (different from local authorities and universities), is a de facto general guideline for public sector accounting. Accruals accounting and auditing

standards for these bodies are laid down in the law with the possibility for the state general accountant to modify them with a simple decree of his/her own. Reference for accounting standards with principles and criteria of the Civil Code applicable to companies, while reference for auditing standards are those set for private companies by the accounting profession.

- In August 2004 a special committee was set up under the auspices of the General State Accounting Department of the Ministry of Economy and Finance. The task is to monitor the evolution of accounting and auditing standards in both private and public sector, and, as a consequence, to propose changes and official interpretations to the current public sector legislation in these fields.

Encouraging further harmonization of accounting standards and related information technology (IT) systems, the Italian National Audit Court has introduced a standardized online system through which regional and local authorities must report their financial accounts.

(d) THE NETHERLANDS. Dutch provinces and municipalities have to comply with the golden rule of public finance, which requires current expense to be defrayed by current revenue. Deficit financing is exclusively allowed for the central government. Therefore Dutch provincial and local governments for a very long time have differentiated between current expenses and capital expenses. They have applied full accrual accounting since the 1980s and prepare balance sheets.

The new accounting system for provinces was introduced in 1979 (effective as of fiscal year 1982), and in 1982 new accounting rules for municipalities were promulgated to take effect in fiscal year 1985. The application of accrual accounting led to the introduction of a balance sheet with the inherent valuation questions, as well as the recognition of payables as cost and of receivables as revenue at year-end. In 1995 new accounting rules were introduced for both provinces and municipalities aimed at improving understanding of the complete condition of a province or a municipality. The reform was based on four basic assumptions:

1. The Civil Law on Financial Reporting, applicable to the private sector, should be used as a reference as much as possible and justifiable under the motto "Harmonize where possible and differentiate where necessary."
2. The democratic principle should be supported along with the constitutional principle of autonomy of the provincial and municipal governments.
3. The rules should be harmonized.
4. The change should increase information value.

The central government does not yet differentiate between current expenses and capital expenses. It is not yet applying accrual accounting, but uses cash and commitments accounting, which is a type of modified cash accounting. The central government had planned to complete the changeover to accrual accounting by 2006.

(e) SPAIN. The basis of the present financial and budgetary accounting system has been laid down in the late 1970s and all through the 1980s. More precisely, the General Budgetary Law issued in 1977 set the foundation from which the current system of governmental accounting in Spain is derived. That piece of legislation introduced the principles of budget preparation, execution, and control and the basis for the development of a new accounting information system.

In 1984 a General Accounting Code for Governmental Entities was approved, with a framework similar to the General Accounting Code for Business Enterprises, issued in 1973; thus it was inspired by the same general accrual-basis principle. In 1986 a royal decree introducing the Accounting and Budgetary Information System was issued, together with the most significant operative and more detailed accounting standards. Notwithstanding the approved legislation, full implementation of new accounting rules at the local level were not applied until 1992.

For the purpose of management and cost accounting of public entities, basic models as well as specific procedures and guidelines have been set up since 1987, especially for national agencies and public universities. However, these management accounting provisions are not compulsory, but voluntarily adopted by the entities.

The Public General Accounting System provides two recording systems completely integrated:

1. Financial accountancy
2. Budgetary accountancy

Financial accountancy applies an accrual-based system. However, the Public General Accounting System takes the economic and legal environment of the public sector into consideration, which determines that the economic revenues and expenses deriving from budget execution must be recorded when the correlative budgetary rights and obligations occur, that is, when the administrative act is dictated. This entails an accrual-basis principle qualified by the significance that budget and lawfulness have in the public sector. Also when recording fixed assets and capital grants, exceptions are applied to the general accrual criterion. Eventually the Public General Accounting System proposes an adjustment at the end of the year for those economic revenues and expenses accrued during the accounting year, even if the administrative act is not dictated yet. There are two kinds of adjustments, which enable achievement of a pure accrual-based accounting:

- On the one hand, all the revenues and expenses already recorded and assigned to the budget, but not totally accrued, must be corrected through the periodification adjustments.
- On the other hand, all the revenues and expenses accrued in the financial sphere, but not yet assigned to the budget (not formalized transactions), must be recorded.

The new framework calls for two profit-and-loss (P&L) statements:

- Net income: the variation in equity as a result of its budgetary and non-budgetary transactions.
- Budgetary P&L: the difference between all the budgetary revenues and expenses realized during the accounting year, excluding those derived from financial liabilities. Budgetary revenue and expenditure account and its notes must be presented following cash-based principles.

In summary, the Spanish public sector accounting system can be defined a modified accrual-based.

(f) UNITED KINGDOM. In the mid-1990s the UK government started its reform process by introducing GAAP-based accounting in National Health Service agencies. Local government had for many years operated a system of partial accrual accounting and budgeting (the main deficiency was in the area of capital accounting and the treatment of stocks, although in the early 1990s this was remedied at the initiative of the accountancy profession).

An initial announcement about the introduction of resource accounting was made in the November 1993 Budget Statement by the Chancellor of the Exchequer (Minister of Finance). In July 1994 a public consultation paper was issued: "Better Accounting for the Taxpayers' Money: Resource Accounting and Budgeting in Government." This consultation paper defined resource accounting and budgeting as follows:

> The term "resource accounting" covers a set of accrual accounting techniques for reporting on the expenditure of United Kingdom central government, comprising departments and their executive agencies including Trading Funds (the departmental boundary), and a framework for analysing expenditure by departmental objective, relating this to outputs wherever possible. "Resource budgeting" covers planning and controlling public expenditure on a resource accounting basis.

In April 2001 the entire government sector moved to a new resource-based financial management system: resource accounting and budgeting (RAB). RAB is an accrual-based approach to government accounting and budgeting, which also reflects Parliamentary control and a move to focus on outputs, rather than inputs. RAB is based on United Kingdom generally accepted accounting practice (United Kingdom GAAP), in particular the accounting and disclosure requirements of the Companies Act 1985 (which applies to private sector companies) and accounting standards, adapted to meet the particular requirements of central government and parliamentary control. The system intends to provide a better picture of the true costs of a department's activities, including use of assets, costs of capital, and noncash costs, and relating these more directly to any revenues generated by the activity. It also aims at improving local accountability capacity for assets and

liabilities of local government units. Each financial year the Treasury updates the accounting guidelines according to the standards set by the UK's Accounting Standards Board. To ensure the correct implementation of new accounting standards, the central government has employed an increasing number of qualified accountants: from nearly 600 in 1989 to 2,200 in 2003.

In 1995, following committee hearings about the Treasury's work to that date on introducing resource accounting and budgeting, two influential committees of the House of Commons—the Treasury Select Committee and the Committee of Public Accounts—recommended that the government consider the case for consolidating departmental resource accounts. In 1997, the government announced its intention of undertaking a study of the merits and feasibility of developing a consolidated set of financial statements for the public sector as a whole—"whole of government accounts." The feasibility study recommended in 1998 that whole of government accounts be produced, based on generally accepted accounting practice in the UK.

In addition to key government planners and managers, other potential users of whole of government accounts are the Parliament and the taxpayers. All central government entities have to present their accounts to Parliament. But Parliament does not receive audited financial statements that provide a true and fair view of the government's overall financial performance, including the extent to which current expenditure has been matched by current income (mainly taxation, of course) and the extent to which the liabilities of government are matched by assets. Whole of government accounts will provide that information, thereby increasing the transparency of the government's accountability to Parliament.

The Treasury is introducing whole of government accounts in two phases: first, consolidated accounts for the central government sector, which we are calling central government accounts, for 2003–2004. Central government bodies in the UK include government departments and their executive agencies, advisory and tribunal nondepartmental public bodies, together comprising the consolidated departmental resource accounts, and executive nondepartmental public bodies, which, with two exceptions, are outside the departmental resource accounting boundary; second, whole of government accounts for 2006–2007 bringing together the central government accounts and the accounts of the remaining public sector entities—National Health Service Trusts, public corporations, and local government—thus consolidating over 1,800 organizations. There are still some divergences on the public corporation and local government sectors—mainly related to fair value accounting for fixed assets and, in local government, accounting for infrastructure assets such as roads. The Treasury has been working closely with the Chartered Institute of Public Finance and Accountancy and colleagues in Scotland (who are responsible for setting accounting policies for local authorities) to bring about convergence of local government accounting.

The UK government is also working on a new reporting regime for local councils. Every council will be required to produce an annual statement on

efficiency savings; the new annual efficiency statements will also require councils to differentiate between cashable and noncashable savings. This additional requirement is strictly related to new efficiency targets introduced by the Gershon Efficiency Review. In mid-2004, the Gershon Efficiency Review identified £20 billion of "auditable and transparent efficiency gains" to be achieved in 2007–2008 across the public service. The study identified seven areas where the public sector should focus to gain the £20 billion: back-office functions; procurement; transactional services; policy, funding, and regulation of devolved public services; policy, funding, and regulation of the private sector; productive time; and relocation. Under the Efficiency Review, local government is expected to deliver total efficiency gains of £6.45 billion by 2007–2008, representing savings of 2.5 percent a year, of which at least half will need to be cash-releasing.

69.5 CONCLUSIONS

The public sector move is surely recognized as beneficial; nonetheless the process requires the utmost care to make sure it is thoroughly implemented and open issues are resolved. The difficulty of finding the optimal approach is clearly demonstrated by the current mix of full cash-based, modified cash-based, modified accrual-based, and full accrual-based financial accounting and budgeting solutions that various governments have adopted.

- Establishing internationally agreed accounting standards will be helpful to make sure uncertainty is reduced in the evaluation of assets, liabilities, purchasing power parities (PPPs), and so on.
- Harmonizing principles between financial accounting and budgeting will be paramount. It is technically and politically difficult for government organizations that are funded by taxation to establish a relationship between inputs, outputs, and outcomes. Essentially, the budget is the main tool to assess performance and control finances. The focus of current accounting standards is exclusively on financial reporting, not on budgeting. That means if accruals are applied only to the government accounts and not to the budget, the financial reports would not be taken seriously; the budget is still the key management document in the public sector and accountability is based on implementing the budget as approved by the legislature. To avoid the risk of an accrual financial report becoming a purely technical accounting exercise, there are several solutions: The budget should be prepared on an accrual basis according to government information on accruals, the budget and financial reports should be harmonized effectively, and other measures should be taken to make effective use of accounting information on an accrual basis.
- Implementing accrual accounting as a component of the overall government modernization process. Accrual is meant to improve the decision

making process; thus it will be essential to accompany it with cultural changes; to match accountability, responsibility, and performance incentives; to ensure proper audit from National Audit Offices; to grow skills; and to involve all stakeholders in the early stages.

Leveraging on cross-border experiences will be helpful and must be complemented by careful planning of the migration.

69.6 APPENDIX

What Types of Appropriation Are Used in the Budget?	A	B	C	D
Austria		X		
Belgium	X	X		
Czech Republic		X		
Denmark	X	X		
Finland	X			X
France				
Germany		X		
Greece		X		
Hungary	X	X		
Ireland		X		
Italy	X			X
Netherlands	X			X
Norway		X		
Portugal		X		
Slovak Republic				
Slovenia		X		
Spain		X		
Sweden				X
United Kingdom				X
Australia			X	
Japan		X		
United States	X			

A = Obligation- or commitment-based—right to make commitments in the budget year and make cash payments without a predetermined time limit.
B = Cash-based only—authority to make cash payments over a limited period of time (annually).
C = Accrual-based only—covers the full cost of the operations of a ministry or agency and increases in liabilities or decreases in assets.
D = Both cash and accruals.
Source: OECD/World Bank, 2003.

On what Basis of Accounting Are the Consolidated, Whole of Government Annual Financial Statements?	A	B	C	D	E	E1	E2	E3	E4	F	G
Austria		X									
Belgium		X									
Czech Republic		X									
Denmark	X										
Finland					X						
France	X										
Germany		X									
Greece		X									
Hungary		X									
Ireland			X								
Italy	X										
Netherlands		X									
Norway		X									
Portugal	X										
Slovak Republic		X									
Slovenia		X									
Spain	X										
Sweden					X		X				
United Kingdom	X										X
Australia				X							
Japan	X										X
United States					X		X	X	X		

A = There is no consolidated, whole of government annual financial statement.
B = Full cash basis.
C = Cash basis, except that certain transactions are treated on accrual basis.
D = Full accrual basis only.
E = Full accrual basis except:
E1 = Capital expenditures are treated as ordinary expenditure (i.e., no capitalization or depreciation of assets).
E2 = Tax receipts.
E3 = Land and natural resources.
E4 = Other.
F = Both full cash basis and full accrual basis.
G = Other.
Source: OECD/World Bank, 2003.

If Applicable, on what Basis of Accounting Are Government Organization Annual Financial Statements?	A	B	C	D	D1	D2	D3	D4	E	F
Austria										
Belgium	X									
Czech Republic	X									
Denmark		X								
Finland				X						
France										
Germany	X									
Greece	X									
Hungary		X								
Ireland										
Italy									X	
Netherlands			X							
Norway	X									
Portugal									X	
Slovak Republic	X									
Slovenia		X								
Spain	X									X
Sweden			X							
UK	X									X
Australia			X							
Japan	X									X
United States				X		X	X	X		

A = Full cash basis.
B = Cash basis, except that certain transactions are treated on accrual basis.
C = Full accrual basis only.
D = Full accrual basis except:
D1 = Capital expenditures are treated as ordinary expenditure (i.e., no capitalization or depreciation of assets).
D2 = Tax receipts.
D3 = Land and natural resources.
D4 = Other.
E = Both full cash basis and full accrual basis.
F = Other.
Source: OECD/World Bank, 2003.

References

Accounting framework for the European Communities: Modernisation of the Accounts. 2001. Working Paper, June.

Adhémar, Philippe. n.d. IFAC Public Sector Committee: Update on PSC's activities and output from September 2003 to 2004. Speech for the Joint European Commission/FEE meeting by Philippe Adhémar (chairman, PSC).

Adhémar, Philippe. 2006. International Public Sector Accounting Standards Board. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Philippe Adhémar (IPSASB chair).

Baltzersen, Morten. 2006. Public-private partnerships. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Morten Baltzersen (Norwegian Ministry of Finance).

Carruthers. Ian. 2006. Integrating accrual cost and performance information. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Ian Carruthers (HM Treasury).

Caumeil, Alain. 2006. La reforme comptable et la preparation de la certification des comptes de l'etat en France. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Alain Caumeil (MINEFI—direction générale de la comptabilité publique).

Comes, Wendy M. 2006. FASAB's conceptual framework. Presentation at the Sixth Annual OECD Public Sector Accruals Symposium, March.

Conclusions of the conference on accrual accounting in the public sector by Deputy Director-General Accounting Officer of the Commission, September 2004.

Devlin, David. n.d. Closing address for the Joint European Commission/FEE meeting by David Devlin (president of FEE).

Dublin, Keith. 2006. Using the GFSM 2001 statistical framework to strengthen fiscal analysis. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Keith Dublin (IMF statistics department, government finance statistics).

European Commission. 2002. Commission adopts ambitious action plan to implement full accrual accounting by 2005. Communication of the European Commission, December.

European Commission. 2004. Report on progress at 30 June 2004 of the modernization of the accounting system of the European Commission. Communication from the European Commission, August.

Fallov, Jonas. 2006. The move to accruals: Experiences from Denmark. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Jonas Fallov (head of division).

FEE. 2003. The adoption of accrual accounting and budgeting by governments (central, federal, regional and local). Fédérations des Experts Comptables Européens (FEE), July.

Fernández-Canteli, Hernández. 2004. Key themes for introducing accrual accounting: Implementation, including embedding in administrative procedures and IT solutions; also challenges and pitfalls of the transition to accruals. Speech for the Joint European Commission/FEE meeting, September.

Gibson, Peter. 2006. Integrating of accrual cost information with performance information. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Peter Gibson (assistant secretary, accounting policy, Department of Finance and Administration, Australia).

Hepworth, Noel. 2003. Accrual accounting in the public sector. CEF Conference, Slovenia, presentation by Noel Hepworth (Chartered Institute of Public Finance and Accountancy, UK).

Hickey, Liz. 2006. International accounting standard setting. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Liz Hickey (director of technical activities, IASB).

IFAC. 2006a. *IFAC handbook of International Public Sector Accounting Standards Board pronouncements*. IFAC.

IFAC. 2006b. IPSAS adoption by governments. IFAC, March.

Jones, Rowan. 2004. Why accrual accounting? Speech for the Joint European Commission/FEE meeting by Rowan Jones (University of Birmingham and chair of Comparative International Governmental Accounting Research Network [CIGAR]), September.

Laliberté, Lucie, Paul Sutcliffe, and Jean-Pierre Dupuis. 2006. Task Force on Harmonization of Public Sector Accounting (TFHPSA) progress report. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Lucie Laliberté (chair, TFHPSA), Paul Sutcliffe (chair, WG I), and Jean-Pierre Dupuis (WG II).

Lüder, Klaus. n.d. Accrual accounting in central government: Where are we now? Speech for the Joint European Commission/FEE meeting by Klaus Lüder, Emeritus Professor of Public Sector Financial Management, University of Speyer, Germany.

Magnússon, Jón. 2006. The Icelandic modified accrual accounting and budgeting experience. Sixth Annual OECD Public Sector Accruals Symposium, March. Presentation by Jón Magnússon (financial management department, Ministry of Finance).

Mawhood, Caroline. 2004. Accrual accounting in the public sector: Progress and achievements. Introductory speech for the Joint European Commission/FEE meeting, September.

Models of public budgeting and accounting reform. 2002. *OECD Journal on Budgeting* 2/Supplement 1.

OECD/World Bank Budget Practices and Procedures database. www.oecd.org/document/61/0,2340,en_2649_34119_2494461_1_1_1_1,00.html.

Schreyer, Michaele. 2004. Accrual accounting in the public sector: Progress and achievements. Speech for the Joint European Commission/FEE meeting by Michaele Schreyer (member of the European Commission), September.

Shi, Yinghua. 2005. Accrual reform in the public sector in China. Stanford Center for International Development, August.

Simpkins, Kevin. 2006. The IASB/FASB conceptual framework project, a public sector perspective. Sixth Annual OECD Public Sector Accruals Symposium, March.

Vareille, Lionel, and David Litvan. 2004. Comptabilité d'Exercice: le cas de la France. Speech for the Joint European Commission/FEE meeting by Lionel Vareille (Direction de la Réforme Budgétaire) and David Litvan (Direction Générale de la Comptabilité Publique), September.

Vogelpoth, Norbert. 2004. Statement on how Germany has applied standards for accrual accounting. Speech for the Joint European Commission/FEE meeting by Norbert Vogelpoth (PricewaterhousCoopers), September.

Watkins, David. n.d. Consolidation of whole of government accounts in the United Kingdom. Speech for the Joint European Commission/FEE meeting by David Watkins (HM Treasury).

Zambon, Stefano. 2004. In the midst of change: Accounting standards for public administrations in Italy? Speech for the Joint European Commission/FEE meeting by Stefano Zambon (Università di Ferrara, director of CIRAMAP), September.

CHAPTER 70

INTRODUCTION TO CHINA'S BANKING SECTOR

Anthony Tarantino, PhD

70.1 INTRODUCTION

Comprehending China's banking sector is essential in understanding its corporate governance and economic future. The banking sector dominates China's financial system, is very important to its overall economy, and will be a role model for other Chinese industries to follow in improving corporate governance. China's bank deposits are massive at $3.5 trillion and represent 160 percent of gross domestic product (GDP)—the highest in the world. As a comparison, Japan stands at 145 percent, the United Kingdom at 107 percent, the United States at 77 percent, and India at 68 percent.[1]

China's banking system is growing and improving at an impressive rate, but has a way to go to address institutional, organizational, and political problems in order to achieve parity with international financial institutions. A key problem is the inability of many banks to reduce the large numbers of nonperforming loans (NPLs). China's banks offer loans at unrealistically low rates, which has encouraged overinvestments in many sectors of the economy. These inefficiencies have been estimated to cost the Chinese economy about $25 billion per year.[2]

China's desire to meet the Basel II requirements may offer the best hope of bringing China's banking sector up to international standards. It is only because

of the sustained high growth rates of the Chinese economy that its banking sector has been able to avoid a financial crisis over its systemic weaknesses and inefficiencies. These problems stifle economic growth by propping up inefficient enterprises and denying funds to the most efficient enterprises. McKinsey and Company estimates that fixing these shortcomings would raise GDP by 13 percent or over $250 billion.[3]

70.2 CHINA'S BANKING REGULATORY ENVIRONMENT

When China entered the 1980s and embraced Western-style corporations, it had only three banks: the People's Bank of China (PBC), the Bank of China (BOC), and the China Construction Bank (CCB).

In the 1980s a series of reforms resulted in the following changes:

- The BOC and CCB statuses were upgraded.
- The Agricultural Bank of China was formed.
- The Industrial and Commercial Bank of China (ICBC), which is now the largest of the state-owned banks, took on the commercial banking functions of the PBC.
- The PBC has become China's central bank.
- New commercial banks were formed, almost all state-owned.[4]

The Big Four banks (BOC, CCB, Agricultural Bank of China, and ICBC) dominate China's banking sector and account for over half of banking assets. As a group, they face many challenges common in emerging markets, such as nonperforming loans, as well as challenges unique to China's central and market hybrid, such as pressure to support dysfunctional state-owned enterprises (SOEs), which created a bad-debt burden. Historically, China's banks have not been free to price loans based on risk levels. In the past few years, consumer lending has risen and now represents about 10 percent of all loans.

There has been a reduction in government interference in making loan decisions and support for reducing nonperforming loans (NPLs) by recapitalizing state-owned banks. This has resulted in removing over $330 billion in NPLs. The government is also encouraging internal reforms to reduce operating costs.[5]

In a major step toward modernization, the government has supported foreign banks taking a stake in government-owned banks. This has many benefits, including raising their internal risk management standards and exposing them to more advanced management techniques and the latest technology developments. Foreign bank investment hit about $18 billion in 2005 with Bank of America, Goldman Sachs, HSBC, and Royal Bank of Scotland taking leading roles. Regulations currently restrict foreign ownership to 20 percent of assets.[6]

Three of the Big Four banks are now listed on foreign stock exchanges:

- October 2005, China Construction Bank (CCB)—raising $8 billion
- May 2006, Bank of China (BOC)—raising $9.7 billion

- October 2006, the Industrial and Commercial Bank of China (ICBC)—raising $22 billion, the world's largest initial public offering (IPO) up to that time

A major driver of banking reform has been China's membership in the World Trade Organization (WTO). This had led to removing functional and geographical restrictions, but foreign banks still suffer through bureaucratic licensing requirements, making expansion a challenge. Foreign banks need to incorporate locally in order to maximize their access to markets, which has the effect of encouraging additional collaboration with Chinese banks.

70.3 FITCH'S EVALUATION OF CHINESE BANKS

According to the Fitch Ratings service, there has been significant progress in reforming Chinese banks in the past few years. Most large banks are reporting nonperforming loan (NPL) ratios under 5 percent, and more than 20 of them have partnering agreements with foreign banks. Fitch is also encouraged by the number of successful IPOs.[7]

But Fitch is concerned that many areas require improvement and that reforms are externally driven, such as recapitalization and NPL carve-outs by the government, and financial transparency by the IPO process. In other words, there is no culture of compliance in most banks. The more difficult reforms remain (overall credit culture, risk management, and corporate governance), which causes Fitch to raise warning flags. As a result, Fitch increased its ratings for only one Chinese bank, ICBC, and then only after its IPO.[8]

Fitch notes that state support for Chinese banks remains strong but is inconsistently applied depending on the relationships involved more than any set of regulations. Fitch is not concerned about compensation for individual depositors, but does have concerns about compensation for other creditors. As a result, Fitch is not changing its support ratings.

Fitch is projecting broad-based improvements in 2007, but exceptions are likely as second-tier banks restructure and the interest rate spread between them and large banks widens. Other areas of concern include increased foreign bank competition, high levels of excess liquidity, and growing disintermediation (removal of the middleman).

The performances of Chinese banks continue to improve, supported by recent reform, but remain weak when compared to their international peers. Chinese banks operate in an environment of high operational risk and have prospered due to the sustained high growth of China's economy, not by processes controlled by the banks. Fitch notes that lending by the Big Four Chinese banks, which account for over half of all bank assets, was strong in 2006, but Chinese officials are increasingly pressuring them to slow down their lending over fears that China's economy is growing too rapidly.[9]

70.4 CHINA'S BANKING REGULATORY AGENCIES

Three government agencies have oversight over the banking industry: the People's Bank of China (PBC), the China Banking Regulatory Commission (CBRC), and the China Securities Regulatory Commission (CSRC).

These agencies administer the following laws and regulations:

- Administrative Rules for Financial Statistics
- Administrative Rules for RMB Bank Settlement Accounts
- Administrative Rules for the Reporting by Financial Institutions of Large-Value and Suspicious Foreign Exchange Transactions
- Administrative Rules for the Reporting of Large-Value and Suspicious RMB Payment Transactions
- Administrative Rules Governing the Equity Investment in Chinese Financial Institutions by Overseas Financial Institutions
- Administrative Rules of the People's Bank of China for the Seizure and Verification of Counterfeit Currency
- Code of Corporate Governance for Listed Companies in China
- Guidelines on Corporate Governance Reforms and Supervision of the Bank of China and Construction Bank of China
- Insurance Law of the People's Republic of China
- Law of the People's Republic of China on Banking Regulation and Supervision
- Law of the People's Republic of China on Commercial Banks
- Measures Governing the Statistics and Declaration of International Receipts and Payments
- Provisional Administrative Rules Governing Derivatives Activities of Financial Institutions
- Provisional Procedures for Designated Bank's Purchase and Sale of Foreign Exchange
- Provisional Risk Assessment System for Joint-Stock Commercial Banks
- Provisional Rules for Security Protection of Financial Institution Computer Information System
- Regulation Governing Capital Adequacy of Commercial Banks
- Regulations on Closure of Financial Institutions
- Rules for Anti-Money Laundering by Financial Institutions
- Securities Law of the People's Republic of China

Historically, all transactional and financial data within and among banks and their customers were not owned by the banks, but by the Chinese government and administered by the CBRC and PBC. This is now changing to be in better alignment with international banking best practices and frameworks, such as the Basel accords.

70.5 THE PEOPLE'S BANK OF CHINA (PBC)

The People's Bank of China (PBC) acts as China's central bank. It is charged with developing and implementing sound monetary policies that will assure stability and confidence in the financial industry, while protecting investors and other stakeholders. The PBC was created in 1948, one year prior to the 1949 founding of the People's Republic of China. The PBC is comprised of 13 functional departments, and its primary functions include:

- Formulating and implementing monetary policy
- Issuing and administering the circulation of the currency
- Licensing and supervising financial institutions
- Regulating all financial markets
- Managing official foreign exchange and gold reserves; acting as fiscal agent for the government
- Maintaining payment and settlement systems and their integrity
- Collecting and analyzing financial statistical data from banks
- Participating in international financial activities in the capacity of the central bank
- Overseeing the State Administration of Foreign Exchange[10]

70.6 CHINA BANKING REGULATORY COMMISSION (CBRC)

Established in 2003, the CBRC regulates the domestic banking industry. The responsibilities of the CBRC's major departments include:

- *Banking Supervision Department I* —responsible for the supervision of state-owned commercial banks and asset management companies
- *Banking Supervision Department II* —responsible for the supervision of equity-holding commercial banks and city commercial banks
- *Banking Supervision Department III* —responsible for the supervision of policy banks, postal savings institutions, and foreign banks
- *Non-Bank Financial Institutions Supervision Department* —responsible for the supervision of nonbank financial institutions (excluding those conducting securities, futures, and insurance businesses)
- *Cooperative Finance Supervision Department* —responsible for the supervision of rural and urban credit cooperatives[11]

The scope of the CSRC's oversights includes the following entities:

- The Big Four banks
- Three policy lenders
- Eleven national shareholding banks
- Four state-owned asset management companies
- Over 100 city commercial banks
- Thousands of credit unions[12]

The CBRC has been responsible for the enactment of milestone regulations, with the goal of expanding China's banking markets. The functions of the CBRC include:

- Formulate supervisory rules and regulations governing the banking institutions
- Authorize the establishment, changes, termination, and business scope of the banking institutions
- Conduct on-site examination and off-site surveillance of the banking institutions, and take enforcement actions against rule-breaking behaviors
- Conduct "fit and proper" tests on the senior managerial personnel of the banking institutions
- Compile and publish statistics and reports of the overall banking industry in accordance with relevant regulations
- Provide proposals on the resolution of problem deposit-taking institutions in consultation with relevant regulatory authorities

The regulatory objectives of the CBRC include:

- Protect the interests of depositors and consumers through prudential and effective supervision
- Maintain market confidence through prudential and effective supervision
- Enhance public knowledge of modern finance though customer education and information disclosure
- Combat financial crimes—anti-money laundering, bribery and corruption, and terrorist financial transactions prevention
- Prevent systemic risks in the banking systems
- Monitor implementation of the policies of the PBC and other regulatory agencies[13]

CBRC Support for Basel II Capital Accords. As part of the process for preparing China's major banks for the Basel II capital accords, the CBRC is moving quickly to bring about improved domestic banking operations, processes, and controls to be in line with international standards. The CBRC has a very aggressive goal of bringing Chinese banks in line with Basel II requirements by 2009. This will require very fundamental changes in infrastructure and processes:

- Much greater internal controls
- Much more robust corporate governance
- Enhanced supervisory transparency to meet International Accounting Standards (IAS) and International Financial Reporting Standards (IFRS) standards

70.7 CHINA SECURITIES REGULATORY COMMISSION (CSRC)

Formed in 1992, the CSRC is the centralized market regulatory governing body in China. The CSRC regulates the securities markets, including the Shenzhen and Shanghai exchanges. Basic functions of the CSRC include:

- To establish a centralized supervisory system for securities and futures markets and to assume direct leadership over securities and futures market supervisory bodies
- To strengthen the supervision over securities and futures business, stock and futures exchange markets, the listed companies, fund management companies investing in the securities, securities and futures investment consulting firms, and other intermediaries involved in the securities and futures business
- To raise the standard of information disclosure
- To increase the ability to prevent and handle financial crises
- To organize the drafting of laws and regulations for securities markets
- To study and formulate the principles, policies, and rules related to securities markets
- To formulate development plans and annual plans for securities markets
- To direct, coordinate, supervise, and examine matters related to securities in various regions and relevant departments
- To direct, plan, and coordinate test operations of futures markets
- To exercise centralized supervision of securities business[14]

Major responsibilities of the CSRC include:

- Studying and formulating policies and development plans regarding securities and futures markets, drafting relevant laws and regulations on securities and futures markets, and working out relevant rules on securities and futures markets
- Supervising securities and futures markets and exercising vertical power of authority over regional and provincial supervisory institutions of the market
- Overseeing the issuance, trading, custody, and settlement of equity shares, convertible bonds, and securities investment funds; approving the listing of corporate bonds; and supervising the trading activities of listed government and corporate bonds
- Supervising the listing, trading, and settlement of domestic futures contracts, and monitoring domestic institutions engaged in overseas futures businesses in accordance with relevant regulations
- Supervising the behavior of listed companies and their shareholders who are liable for relevant information disclosure in securities markets

- Supervising securities and futures exchanges and their senior management in accordance with relevant regulations, and securities associations in the capacity of the competent authorities
- Supervising securities and futures companies, securities investment fund managers, securities registration and settlement companies, futures settlement institutions, and securities and futures investment consulting institutions; approving in conjunction with the People's Bank of China the qualification of fund custody institutions and supervising their fund custody business; formulating and implementing rules on the qualification of senior management for the aforementioned institutions; and granting qualification of the people engaged in securities and futures-related business
- Supervising direct or indirect issuance and listing of shares overseas by domestic enterprises, supervising the establishment of securities institutions overseas by domestic institutions, and supervising the establishment of domestic securities institutions by overseas organizations
- Supervising information disclosure and proliferation related to securities and futures and being responsible for the statistics and information resources management for securities and futures markets
- Granting, in conjunction with relevant authorities, the qualification of law firms, accounting firms, asset appraisal firms, and professionals in these firms, engaged in securities and futures intermediary businesses, and supervising their relevant business activities
- Investigating and penalizing activities violating securities and futures laws and regulations
- Managing the foreign relationships and international cooperation affairs in the capacity of the competent authorities
- Requiring security brokerages to file and publish to their company web sites audited financial results[15]

70.8 CHINA'S ADOPTION OF BASEL II

China is very much committed to meeting the Basel II capital accords, realizing it is the price of admission to global financial markets. To do otherwise would relegate the Chinese financial industry to a second-class status and hurt its cost of raising capital. As a consequence, the government will continue to place pressure on the Big Four banks to improve their processes and restructure their organizations to be in line with international standards. Part of this process included the government's recapitalization of the Big Four banks to prepare them for their IPOs.

As part of the preparation for Basel II, the government is modernizing its security and privacy regulations following ISO standards. Traditionally, the government has permitted data to be processed offshore for global banks but not for Chinese banks. Global banks and their suppliers must demonstrate that ability

to re-create master level and transactional level on demand. The CBRC reserves the right to audit any of these offshore facilities.[16]

Business continuity and resiliency planning will also need to improve to meet Basel requirements and reduce operational risk. To this end, the government is creating a supervisory information system to evaluate risk profiles of major banks and their first-tier suppliers. What follows is a summary of activities underway by the banking regulatory authority under the State Council:

- Creating and publishing on-site examination procedures and then conducting on-site examination of the business operations and risk profiles of banking institutions
- Supervising banking institutions on a consolidated basis and responding, within 30 days, to the proposals of the People's Bank of China for the examination of banking institutions
- Establishing a rating system and an early warning system for the purpose of supervision of banking institutions
- Determining the frequency and scope of on-site examinations based on a bank's risk profile
- Establishing a system to identify and report emergency situations in the banking sector
- Identifying any emergency situations that may result in systemic banking risks, hence causing severe social instability
- Establishing mechanisms to address emergency situations in banks, including formulating contingency plans, designating institutions and staff members, specifying their responsibilities, and stipulating resolution measures and procedures, which will ensure timely and effective resolution of the emergency situations
- Creating standards and then conducting tests for the competence of banking directors and senior managers of banking institutions
- Compiling and publishing the applicable banking statistics and reports
- Engaging in international banking regulatory activities

Notes

1. Diana Farrell, Susan Lund, and Fabrice Morin, "The Promise and Perils of China's Banking System," *McKinsey Quarterly*, July 2006.
2. Ibid.
3. Ibid.
4. The Economist Intelligence Unit, ViewsWire, 27 October 2006.
5. Ibid.
6. Ibid.
7. Fitch Ratings, "Chinese Banks—2006 Ratings Season Review and 2007," December 13, 2006.

8. Ibid.
9. Ibid.
10. See the PBC web site: www.pbc.gov.cn/english/.
11. See the CBRC web site: www.cbrc.gov.cn/.
12. See the CBRC web site: www.cbrc.gov.cn/.
13. See the CSRC web site: www.csrc.gov.cn/n575458/index.html.
14. See the CSRC web site: www.csrc.gov.cn/n575458/index.html.
15. See the CSRC web site: www.csrc.gov.cn/n575458/index.html.
16. See the State Council's web site: http://english.gov.cn/links/statecouncil.htm.

CHAPTER 71

THE KEY TO MALAYSIAN FINANCIAL INSTITUTIONS COMPLIANCE AND ECONOMIC CRIME REQUIREMENTS

Tommy Seah, CFE

71.1 BACKGROUND

On June 27, 2006, at 2:30 PM, the supervision and regulation departments of the central bank of Malaysia, Bank Negara Malaysia (BNM), called for a meeting for all compliance officers from the Composite, Life Business, and Takaful Operators and working group members.

The purpose of the meeting was twofold:

1. To discuss the salient features of the draft Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT)
2. To discuss the salient features of the draft AML/CFT Sectoral Guidelines

The presentation of Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism was conducted by the Financial Intelligence Unit, Bank Negara Malaysia.

The meeting's agenda was:

1. Introduction
2. Applicability
3. Customer acceptance policy
4. Customer due diligence (CDD)
5. Record keeping
6. Ongoing monitoring
7. Reporting mechanism
8. Counter financing of terrorism
9. Penalty for noncompliance

BNM introduced the Guidelines and reiterated that they were issued pursuant to Section 83 of the Anti-Money Laundering Act (AMLA) of 2001, which was established and formulated to address the requirements that must be complied with by the reporting institutions. This is, of course, in accordance with the AMLA and the Financial Action Task Force Against Money Laundering (FATF) Forty Recommendations and Nine Special Recommendations.

The presenter made it exceedingly clear that the requirements apply to all reporting institutions listed in the First Schedule to the AMLA, including its local and foreign branches and subsidiaries carrying on any of the businesses or activities listed in the First Schedule to the AMLA. Where there is conflict between the local and foreign regulatory requirements, the more stringent requirements are to be adopted to the extent that is permitted by the host country's laws and regulations. If, for whatever reasons, it is unable to comply, the financial institution should issue an exception report to the head office.

With regard to customer acceptance policy, the financial institution is to:

- Develop customer acceptance policies and procedures to address the establishment of business relationship with the customer.
- Identify and assess risk of customers.
- Have reasonable measures to address the different risks posed.
- Consider risk profiling factors:
  - Origin of the customer and location of business
  - Background or profile of the customer
  - Nature of the customer's business structure of ownership for a corporate customer
  - Any other information suggesting that the customer is of higher risk
- Continuously monitor the customer's transaction activity pattern to ensure it is in line with the customer profile.

With regard to customer due diligence, the financial institution is to conduct customer due diligence and obtain satisfactory evidence and properly establish

in its records the identity and legal existence of persons applying to do business with the financial institution.

The customer due diligence should be conducted when:

- Establishing a business relationship with the customer
- Carrying out an occasional transaction that involves a sum or wire transfer in excess of the amount specified by Bank Negara Malaysia under its sectoral guidelines or relevant circular
- The reporting institution has any suspicion of money laundering or financing of terrorism
- The reporting institution has any doubts about the veracity or adequacy of previously obtained information

The customer due diligence undertaken by the reporting institution should comprise at least the following actions:

- Identify and verify the person conducting the transaction.
- Identify and verify beneficial ownership and control of such transaction.
- Obtain information on the purpose and intended nature of the business relationship/transaction.
- Conduct ongoing due diligence and scrutiny to ensure the information provided is updated and relevant.

Unwillingness to cooperate may itself be a factor of suspicion. If the customer fails to comply with the customer due diligence requirements, the reporting institution should not commence or complete such business relations.

71.2 CUSTOMER DUE DILIGENCE FOR INDIVIDUAL CUSTOMERS

With individual customers, obtain at least the following information:

- Full name
- NRIC/passport number
- Permanent and mailing address
- Date and place of birth
- Nationality

Substantiate by:

- NRIC for Malaysians/permanent residents
- Passport for foreigners

Where there is doubt, produce other supporting identification documents (with photograph) issued by an official authority.

71.3 CORPORATE CUSTOMERS

For corporate customers, furnish the following documents:

- Memorandum, article, or certificate of incorporation/partnership
- Identification document of directors/shareholders/partners
- Board of directors' or directors' resolution
- Authorization for any person to represent the company or business
- Identification document of authorized person

Where there is doubt:

- Conduct a basic search or enquiry on the background, and/or
- Verify with the Companies Commission of Malaysia.

Understand the ownership and control structure and determine the source(s) of funds.

71.4 CLUBS, SOCIETIES, AND CHARITIES

Clubs, societies, and charities require the following documents:

- Relevant constituent documents (or other similar documents)
- Identification of the office bearer
- Authorization for any person to represent the club, society, or charity

71.5 LEGAL ARRANGEMENT

For legal arrangements, take reasonable measures to:

- Understand the relationships among the relevant parties
- Obtain satisfactory evidence of legal status and the identity of the relevant parties
- Know the nature of their capacity and duties as trustees or nominees

71.6 BENEFICIAL OWNERSHIP AND CONTROL

Conduct customer due diligence on the beneficiary or controller of any transaction where it is suspected the transaction is conducted on someone else's behalf.

71.7 RELIANCE ON INTERMEDIARIES FOR CDD

With intermediaries, the reporting institution must be satisfied that the intermediary:

- Has an adequate customer due diligence (CDD) process
- Has a reliable mechanism to verify customer identity
- Can provide the necessary information and relevant documentation available immediately upon request

- Allows periodic review by the reporting institution to verify the due diligence undertaken
- Where appropriate, is properly regulated and supervised by the respective authorities

71.8 NON-FACE-TO-FACE CUSTOMERS

Reporting institutions should establish business relationships upon completion of the customer due diligence process conducted through face-to-face interaction only.

71.9 POLITICALLY EXPOSED PERSON

With foreign individuals, establish a risk management framework to determine whether current or new customers are politically exposed persons (PEPs). Gather sufficient and appropriate information from the customer and through publicly available information. In addition:

- Establish the source(s) of wealth and funds.
- Have senior management make decisions about whether to enter into business relationships with PEPs.
- Conduct enhanced ongoing due diligence.

71.10 HIGHER-RISK CUSTOMERS

Higher-risk customers require enhanced due diligence, such as obtaining more detailed information from the customer and through publicly available information—in particular, on the purpose of transaction and source of funds. It is important to obtain approval from senior management of the reporting institution at the head office before establishing the business relationship with the customer.

Examples of higher-risk customers are:

- High-net-worth individuals
- Nonresident customers
- People from locations known for a high crime rate (e.g., drug producing, drug trafficking, smuggling)
- Individuals from countries or jurisdictions with inadequate AML/CFT laws and regulations such as the noncooperative countries and territories (NCCT)
- PEPs
- Customers with legal arrangements that are complex (e.g., trust, nominee)
- Cash-based businesses
- Unregulated industries

71.11 EXISTING CUSTOMERS

With existing customers, ensure that their records, including their customer profiles, remain updated, relevant, and in compliance with the reporting institution's current customer due diligence standards.

Reviews could, at least, be conducted when:

- A significant transaction is to take place.
- There is a material change in the way the account is operated.
- The customer's documentation standards change substantially.
- The reporting institution discovers that the information held on the customer is insufficient.
- Existing customers are considered to be of higher risk.

71.12 RECORD KEEPING

Keep all records and documents with regard to transactions conducted and customer due diligence for at least six years after the transaction has been completed or the business relations with the customer have ended.

Where the records are subjected to an ongoing investigation or prosecution, they should be retained beyond the stipulated retention period as specified.

71.13 COMBATING TERRORISM

In the case of combating financing terrorists, the financial institution is to:

- Maintain a database of names and particulars of terrorists in the Consolidated List and Gazette Orders issued under Section 66C of the AMLA.
- Ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees.
- Regularly check the names of new and existing customers against the names in the database.
- If there is a match, take reasonable and appropriate measures to verify and confirm the identity of the customer.
- Upon confirmation, immediately inform Bank Negara Malaysia and other relevant authorities and freeze or reject the customer's transaction.

CHAPTER 72

CORPORATE GOVERNANCE AND RISK MANAGEMENT IN THE SOUTH AFRICAN BANKING INDUSTRY

Jackie Young

South Africa has been called the "Hub of Africa" because so many financial and business transactions flow through the country from the rest of the continent. The major South African banks have developed a vast outreach, and now provide a service to many other countries in Africa and elsewhere. However, at the same time, it is important to demonstrate a solid commitment to good corporate governance practices. Essentially, this entails that South African banks should think how they must approach and attain a reputable and beneficial framework of corporate governance that is aligned with the basic guidelines and requirements thereof. This includes a sound approach to risk management.

This chapter aims to discuss basic concepts of corporate governance and risk management within the African environment with specific reference to the South African banking industry.

72.1 INTRODUCTION

Most South African banks have accepted operational risk as a major risk type that must be managed. This decision was enhanced by a number of major events and developments on an international front. Of these, the following played a major role in the decision to embed a formal operational risk management framework:

- The 9/11 terrorist attack on the World Trade Center in 2001
- The development of capital requirements for operational risk by the Basel Committee on Banking Supervision during 2003
- The King Committee's Report on Risk and Corporate Governance of 2002
- Various technological developments such as Internet banking and telephone banking
- A general increase in crimes such as money laundering, corruption, fraud, and robberies

In terms of the aforementioned events and developments, the banking industry's operational risk exposures and regulatory responsibilities increased significantly and subsequently forced banks to change their approach to operational risk management to a more proactive management style. From a corporate governance perspective, the South African government and the central bank (South African Reserve Bank) are involved in improving risk management to ensure a healthy banking industry and national economic performance.

72.2 CORPORATE GOVERNANCE

Corporate governance as well as operational risk management are fairly new disciplines that only recently emerged as disciplines in their own right, with many countries, including South Africa, giving them a rightful place as critical determinants in an organization's management structure. According to the United Nations Economic Commission for Africa (UNECA) (2002, 2), good corporate governance exists in those economies where the institutions of government:

- Have the capacity to manage resources efficiently
- Can formulate, implement, and enforce sound policies and regulations
- Can be monitored and be held accountable
- Have respect for the rules and norms of economic interaction

and

- In which economic activity is unimpeded by corruption and other activities inconsistent with the public trust

As such, from a government perspective, the key elements contributing to an environment of good corporate governance are:

- Transparency
- An enabling environment for private sector development and growth
- Institutional development and effectiveness (UNECA 2002, 2)

According to UNECA (2002, 3), in recognition that the responsibility for governance issues lies first and foremost with the national authorities, African states must commit to improving economic governance, for the following reasons:

- To enhance the ability to implement development and poverty reduction policies with scarce resources
- To execute public management functions in an accountable manner
- To create a credible policy environment in which domestic and international investors can have confidence and trade can be enhanced
- To strengthen absorptive capacity to attract and mobilize development assistance flows
- To demonstrate transparent and participatory economic policy making and execution as well as an open flow of information available to all stakeholders
- To signal an adherence to standards of institutional functioning free of corruption

The South African banking industry plays a major and imperative part in these reasons for achieving sound corporate governance, which will also lead to a number of benefits, for example:

- Maximizing the gains from globalization
- Accelerating economic growth
- Reducing poverty
- Creating a more stable, predictable macroeconomic environment

Considering each of the aforementioned reasons in more detail, it is clear that if these reasons are ignored, it could lead to some sort of operational risk for banks, which could have a negative influence on a bank's business growth and development and ultimately shareholder value. For example, the current political situation in South Africa shows a negative trend in coping with the increase in crime and serious offenses. An example is a 42 percent increase in armed robberies in the past financial year (2005/06) in some of the major cities of South Africa, as published in the *Pretoria News* dated September 30, 2006. There has been an increase in other serious crime incidents reported, for example murder, rape, attempted murder, carjacking, and so on. A potential result could be that investors will be hesitant to invest in South Africa, resulting in a negative economic growth, increase in poverty, and not benefiting from globalization. As such, it is clear that if these negative criminal offenses increase, South Africa's future economic growth is seriously being threatened.

Furthermore, a corporate governance issue that could pose a serious risk for South African business, including the banking industry, is the judicial system. Good corporate governance requires an independent judicial system that is impartial, is free from interference, and renders respected judicial decisions. The recent event where Tony Yengeni, a senior political figure, was sentenced to prison for corruption and was escorted to prison by senior members of parliament, indicated some sort of disrespect for the judicial system, reflecting a negative image and a high risk to potential investors.

72.3 OPERATIONAL RISK

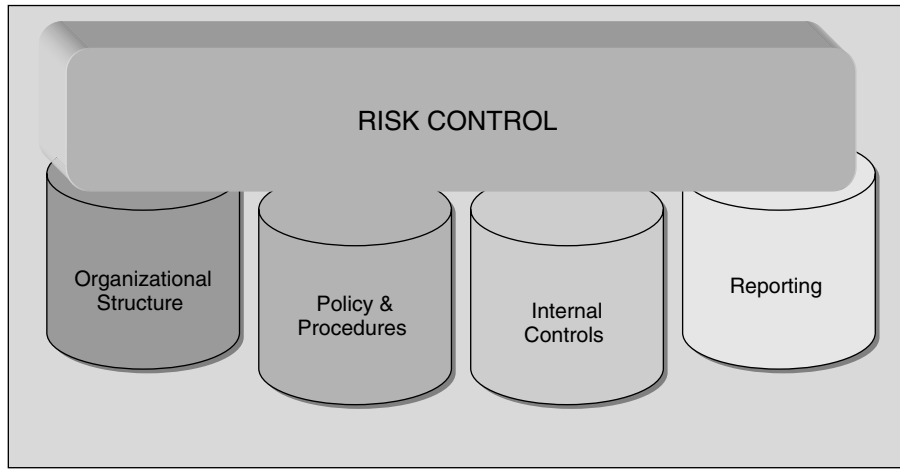
Operational risk is broadly defined as the exposure of an organization to potential losses resulting from shortcomings and/or failures in the execution of its operations. These losses may be caused by internal failures or shortcomings of people, processes, and systems, as well as the inability of people, processes, and systems to cope with the adverse effects of external events (Young 2006, 11). When analyzing this definition, it is clear that the underlying risk factors for operational risk are people, processes, systems, and external events. To address these risk factors, it is imperative to analyze the cause of the risk exposure and to develop and implement subsequent mitigating and control measures.

According to Young (2006, 94), control measures for operational risk are based on four pillars, illustrated in Exhibit 72.1.

The organizational structure will ensure that specific roles and responsibilities are allocated for effective operational risk management, which is a specific corporate governance requirement for risk management.

Policies and procedures is the second pillar, which is imperative for risk management in order to provide consistency and discipline within an organization and ensure the overall defining and allocating of specific roles and responsibilities for managing risk.

Internal controls should be established to ensure the effectiveness of policies and procedures, which is another good corporate governance requirement. The Basel Committee identified, for example, five types of control breakdowns that have led to substantial losses for banks:



Source: Young (2006, 94).

EXHIBIT 72.1 PILLARS OF RISK CONTROL

1. A lack of adequate management supervision and accountability and failure to develop a strong risk management culture within the bank
2. Inadequate assessment of the risk of certain banking activities, whether on- or off-balance sheet
3. The absence or failure of key control activities, such as segregation of duties, approvals, verifications, reconciliations, and reviews of operating performance
4. Inadequate communication of information between levels of management within the bank, especially in the upward communication of problems
5. Inadequate or ineffective audit programs and other monitoring activities

These control breakdowns are typically issues that a well-structured corporate governance and risk management framework will address.

Risk reporting is the fourth risk control pillar and is the process whereby an organization reports on risk internally, through its management information system, and externally, to its regulators and shareholders (Young 2006, 100). This is also an important corporate governance requirement that will assist in effective decision making. According to UNECA (2002, 12), a major element of good corporate governance is effective participatory decision making. This issue poses a risk to a number of African countries when considering, for example, the local elections. It is stated that the smooth running of elections is still problematic in several African countries, with scores of people invariably being disenfranchised, leading to poor risk management and corporate governance (UNECA 2002, 12).

72.4 KING COMMITTEE ON CORPORATE GOVERNANCE

Corporate governance refers to the mechanisms through which a bank and its management are governed. Good corporate governance is a key structural and institutional feature of a functioning market economy. Many developing and transitional economies, such as South Africa, recognize the fact that a healthy and competitive corporate sector is necessary for their sustainable and shared growth and that corporate governance is fundamental for the private sector. As South Africa and other African countries endeavor to attract a share of foreign investments, they have to assure investors that their investments will be secure and efficiently managed on the basis of a transparent and accountable process. Effective risk management can be regarded as one method of providing assurance of a sound investment to investors. A South African initiative to develop a corporate governance framework for risk management was launched during 2002 in the form of the King Committee on Corporate Governance. The purpose of the King Committee was to promote the highest standards of corporate governance in South Africa, which includes the banking industry. According to the report by the King Committee (2002, 96), risk frameworks, as part of an organization's corporate governance, must provide assurance with regard to:

- Effectiveness and efficiency of operations

- Safeguarding of assets
- Compliance with applicable law
- Business sustainability
- Reliability of reporting
- Behaving responsibly toward stakeholders

In terms of risk management, the King Committee (2002, 98) states that the board is responsible for:

- Ensuring that processes and outcomes of key risk indicators are undertaken on an annual basis
- Appointing a board committee or an appointed dedicated committee that should review the risk management process and the significant risks facing the company
- Disclosing risk management in the annual report
- Ensuring that the internal audit function provides an independent assurance that the internal controls ensure effective risk management
- Ensuring that there is compliance with the applicable regulations

Considering the aforementioned and comparing it with the requirements of good corporate governance (namely, that it involves a set of relationships between an organization's management, its board, its shareholders, and its other stakeholders and provides the structure through which the objectives and the monitoring of performance are determined), it is evident that there is a direct correlation between effective risk management and corporate governance. Exhibit 72.2 illustrates the links between the components of good corporate governance and effective operational risk management.

It is clear that there are direct links between the components of corporate governance and risk management. It is furthermore evident that if an organization, like a bank, can provide assurance of complying with the aforementioned governance requirements, it would most likely attract the attention of potential investors.

Due to the negative nature of financial positions of emerging market economies, developing countries need to establish good corporate governance mechanisms that inhibit speculative transactions and flows of short-term capital, while at the same time encouraging long-term capital inflows, especially foreign investments. An important mechanism in this instance is to bring the financial sectors up to the standards of new international financial architecture. This would, for example, also improve decision making and create an environment that encourages investment and savings. According to UNECA (2002, 7), good corporate governance contributes to the efficient mobilization and allocation of capital, the efficient monitoring of corporate assets, the effectiveness of overall corporate performance, and improved national economic performance. In this regard and from a banking perspective, the South African Reserve Bank is

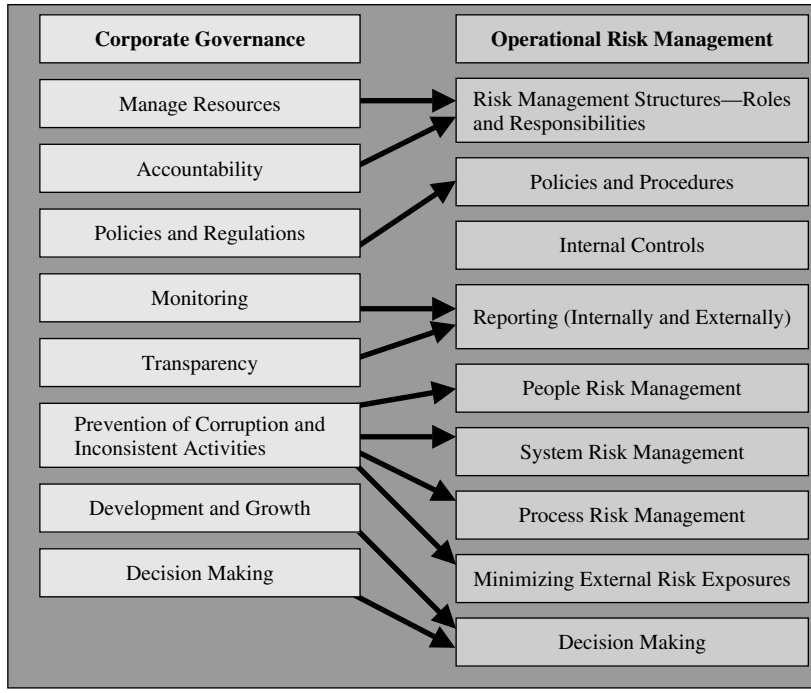


EXHIBIT 72.2 LINKS BETWEEN COMPONENTS OF CORPORATE GOVERNANCE AND RISK MANAGEMENT

taking the lead from the Basel Committee on Banking Supervision to impose a regulatory capital charge for operational risk.

72.5 CAPITAL CHARGE FOR OPERATIONAL RISK

Among the most essential foundations of good corporate governance is the regulatory framework. In most economic sectors, some form of government control is required to deal with potential market failures, including the misuse of market power. According to UNECA (2002, 32), various experiences of the developed countries and the emerging market economies show that the three major areas that have benefited a great deal from a sound regulatory framework are:

1. Securities (capital market)
2. Insurance and banking
3. Monopolistic markets such as utilities

It is thus important that African countries move vigorously to improve their regulatory frameworks in these areas. However, as a result of the transitional state of most African economies and political systems, many African countries are ill

equipped to implement the corporate governance systems that have evolved over centuries in developed market economies. Among the major constraints in this respect are:

- Ownership structure of the corporate sector
- Interlocking relationships with government and the financial sector
- Weak legal and judiciary systems
- Lack of or undeveloped institutions
- Limited human resource capabilities

However, in South Africa there are many initiatives aimed at building good systems of corporate governance and sound principles of risk management, such as the aforementioned King Report published in 2002. Another initiative on the front of risk management is the Basel Committee's proposal for allocating regulatory capital for operational risk.

The South African Reserve Bank is also implementing this initiative for the South African banking industry, which requires banks to use various approaches to calculate a capital charge for operational risk. It varies from a straightforward calculation that is risk-insensitive to more complicated risk-sensitive methods. The aim of calculating a capital charge for operational risk is to protect a bank and the banking industry from collapsing in the event of an unexpected catastrophic incident. In order to use the more advanced method to calculate an accurate capital charge for operational risk, banks are required to comply with specific requirements, such as the following sound risk management principles (aligned with the Basel Committee's proposed principles):

Development of Appropriate Risk Management Environment

- The board should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed.
- The framework for operational risk management should be subject to effective and comprehensive internal audit (the internal audit function should not be directly responsible for operational risk management).
- Senior management should have the responsibility for implementing the operational risk management framework (the framework should be consistently implemented throughout the whole banking organization).
- Senior management should be involved in the operational risk management process by creating an operational risk governance model, including an independent operational risk management function.

Risk Management

- The bank should identify and assess the operational risk inherent in all material products, activities, processes, and systems.

- The bank should implement a process to regularly monitor operational risk profiles and material exposures to losses.
- The bank should have policies, processes, and procedures to control and/or mitigate material operational risks.
- The bank should have in place contingency and business continuity plans to ensure the ability to operate on an ongoing basis and limit losses in the event of severe business disruptions.

DISCLOSURE

- The bank should make sufficient public disclosure to allow market participants to assess their approach to operational risk.
- The operational risk process should be incorporated with other day-to-day processes.
- Top-down and bottom-up communication channels should be established for operational risk.

Once again it is clear that the sound principle for risk management is an initiative to align it with good corporate governance. The South African banks are also very much alert to the influence of good corporate governance and sound risk management on their business. As such they also launched an initiative known as the Financial Sector Charter.

72.6 FINANCIAL SECTOR CHARTER

In August 2002 the South African financial sector committed itself to the development of a Black Economic Empowerment (BEE) charter. This commitment was enacted from January 1, 2004, and will be applied until December 31, 2014; it was made with notice of the following:

- Despite significant progress since the establishment of a democratic government in 1994, South African society remains characterized by racially based income and social services inequalities. This inhibits the country's ability to achieve its full economic potential. Africa is the poorest region in the world and by addressing this issue it will contribute to the reducing of poverty, at least in South Africa, which is also a requirement for good corporate governance.
- BEE is a mechanism aimed at addressing inequalities and mobilizing the energy of all South Africans. It will contribute toward sustained economic growth, development, and social transformation in South Africa. This endeavor will ensure good corporate governance, as it will contribute to the efficient mobilization and allocation of capital, the efficient monitoring of corporate assets, the effectiveness of overall corporate performance, and improved economic performance.

- Inequalities also manifest themselves in the country's financial sector. A positive and proactive response from the sector through the implementation of BEE will further unlock the sector's potential to promote its global competitiveness and enhance its world-class status. Once again this can be related to good corporate governance.
- The financial stability and soundness of the financial sector and its capacity to facilitate domestic and international commerce are central to the successful implementation of BEE. This will also allow the country to exploit the benefits of globalization and creation of a stable macroeconomic environment.

In most economies the financial sector plays a major role in enhancing growth and development. The South African banking industry, as part of this financial sector, is regarded as world class in terms of its skilled workforce, adequate capital resources, infrastructure, and technology and will have a positive influence on this initiative.

72.7 CONCLUSION

It is evident that by complying with the basic requirements of good corporate governance, any organization will have a structured platform for effective operational risk management. This will ensure efficient mobilization and allocation of capital, the efficient monitoring of corporate assets, the effectiveness of overall corporate performance, and improved national economic performance.

Although African countries across the continent are at various stages of implementing good corporate governance principles, most of these initiatives are being hampered by problems of corruption, inadequate infrastructures, and cumbersome bureaucratic procedures. Corruption can be regarded as one of the factors that restrict effective corporate governance in Africa. Grand corruption, for example, tends to involve leaders, politicians, senior bureaurocrats, and entrepreneurs. This can take many forms, such as bribes—for example, South Africa's defense contracting in 2001 allegedly involving top businessmen and senior politicians.

However, apart from the constraints of complying with good corporate governance principles, the implementation of sound risk management practices, especially in the banking industry, will add value to the initiatives to improve the capacity of South Africa to adapt and apply the relevant codes and standards for sound corporate governance.

References

Basel Committee on Banking Supervision. 2003. *Sound practices for the management and supervision of operational risk*. Basel: Bank for International Settlements [s.n.], February.

Basel Committee on Banking Supervision. 2004. *International convergence of capital measurement and capital standards: A reviewed framework*. Basel: Bank for International Settlements [s.n.], June.

King Committee and Commission on Corporate Governance. 2002. *King 2 report on corporate governance for South Africa: Draft for public comment*. Pretoria: Institute of Directors in Southern Africa.

South African Financial Sector Charter, August 2002.

UNECA. 2002. *Guidelines for enhancing good economic and corporate governance in Africa*. United Nations Economic Commission for Africa.

Young, J. 2006. *Operational risk management: The practical application of a qualitative approach*. Pretoria: Van Schaik Publishers.

CHAPTER 73

MEN BEHAVING BADLY IN BANKING: REVEALING THE IRRELEVANCE OF BEST PRACTICES IN CORPORATE GOVERNANCE

Shann Turnbull

73.1 INTRODUCTION

In 2004, a group of seven (G7) male directors of the largest bank in Australia provided a high-profile example of men behaving badly to "cause detriment to the corporation" in the words of Section 182(1)(b) of Australian Corporation Law (ACL 2001). They illustrated the irrelevance of the so-called best practices in corporate governance.

The National Australia Bank (NAB) Annual Report stated for the fiscal year ending September 2003 that it was ranked among the top 30 most profitable financial services organizations in the world and conformed to the highest standards of corporate governance. As the bank was listed in the United States, it had to comply with the Sarbanes-Oxley Act (SOX) and have a "financial expert" on its board.

In March 2004, a report by the Australian Prudential and Regulatory Authority (APRA 2004) was made public about an $A360 million foreign exchange (FX or forex) loss announced by the bank in January of that year. The report by the banking regulator revealed how the so-called best practices of corporate governance had proven to be impotent in permitting the directors to discover, let alone prevent, fraud. It also illustrated how so-called best practices do not provide a mechanism for board disputes to be mediated efficiently, economically, and effectively, or in private.

The problems at the NAB also support this author's views that so-called best practices in corporate governance can be counterproductive, create hubris, and mislead regulators, investors, and stakeholders into believing that their interests are well protected (Turnbull 2001, 2003, 2004). This is discussed further in the concluding section of this chapter.

The Australian Shareholders Association, a nonprofit membership organization, summed up the problems at the NAB in a May 2004 press release that stated:

> Legitimate shareholder expectations and concerns have been ignored and have been treated with contempt. The board has been focused on issues of individual reputation and prestige at the expense of their responsibilities to shareholders to act in their best interests. Shareholders were disappointed by the lack of accountability for the massive HomeSide losses and the recent forex scandals.

The NAB had incurred a loss of almost $A4 billion in 2001 from its U.S.-based HomeSide mortgage business acquired only four years earlier. Due diligence on the acquisition had been carried out by Chris Lewis, a partner of the bank's external auditor, KPMG. In 2001 Lewis left KPMG to become executive general manager—group risk management of the NAB. No director accepted responsibility for the loss, which was the biggest investment disaster in Australian corporate history at that time. Ironically, the 2004 FX loss, which was only one-tenth of the HomeSide loss, resulted in the phased retirement of the whole board and the external auditor.

In January 2004 when the FX losses were revealed, Cathy Walter, the only woman on the board, proposed that the global audit firm PricewaterhouseCoopers (PwC) be sued. The fees paid to PwC for advice in 2003 were twice as large as the fees paid to its statutory auditor. Jim Power, a PwC partner, had acted as the NAB internal auditor during 2002. He had specifically advised Walter, who was chair of the Audit Committee, that the NAB was not exposed to the risk of FX losses as occurred in another overseas bank earlier that year. The external auditor had raised concerns about the NAB's FX trading in 2001 and 2002.

John Thorn resigned as a partner of PwC in September 2003 to become a director of the NAB and a member of the Audit Committee the following month. The board's Risk Management Committee had been formed by the NAB in August 2003 with the charter of its Audit Committee changed accordingly. But the Risk Management Committee, chaired by Graham Kraehe, had only met once before a junior employee blew the whistle on the hidden FX losses in January 2004.

The G7 ganged up against Walter to protect PwC and themselves in March 2004 by calling an extraordinary general meeting (EGM) of shareholders on May 21 to have Walter removed as a director. Unlike the law in some other countries, ACL allows a single director to requisition an EGM to seek changes in the corporate constitution, review board decisions, and decide on the background

information on the bank. This includes an exhibit that records some milestones in the history of the bank and relevant events of "men behaving badly in banking." The third section describes the emerging problems. How two whistle-blowers initiated renewal of the bank's personnel and culture are presented in the next section. Some concluding remarks are presented in the final section on the irrelevance of so-called best practices in corporate governance to avoid problems, let alone enhance performance.

73.2 BACKGROUND TO THE PROBLEMS

The NAB was founded in Melbourne in 1858 during the blooming of a great gold rush in Australia. Growth was organic until after the Australian states federated in 1901 to form a commonwealth government of Australia. Five banking acquisitions were made from 1918 to 1981, as set out in Exhibit 73.1, to make the NAB a truly national bank.

Australian banks had been tightly regulated by the Reserve Bank of Australia (RBA) until an inquiry into the financial system recommended a more competitive environment in 1981. Until then the RBA had no policy on Australian ownership of an overseas bank. The RBA had never had a request for approving Australian ownership of an overseas bank until the author did in 1970 as the chairman of a publicly traded finance company.

The NAB began expanding its operations overseas in 1987 with a series of acquisitions over the following ten years, as set out in Exhibit 73.1. Don Argus oversaw the acquisitions. His career in banking began when he was 17. He rose up through the ranks to become an NAB director at age 51 in 1989 and CEO in 1992. Also overseeing the overseas acquisitions was Mark Raynor, who was appointed to the board in 1985 as a nonexecutive director. He became chairman at the end of the overseas acquisition period in 1997.

Cathy Walter, a corporate solicitor, joined the board in 1995 as its youngest member, its only lawyer, and the first female. She became a member of the Audit Committee in 1997 and chair of the committee in 2000. In 2000 the Audit Committee had only two other members—Mark Raynor, the board chairman, and Charles Allen, a director appointed in 1992.

It was in late 1997 that the board approved in principle to make a $US1.2 billion acquisition of HomeSide Inc., a U.S. mortgage business. The acquisition was completed in early 1998 after due diligence investigation by Chris Lewis, a partner of global audit firm KPMG, the statutory external auditor of the NAB. Another executive involved in the acquisition, Frank Cicutto, joined Don Argus on the board in 1998. Like Argus, Cicutto had spent a lifetime with the bank, having been first employed in 1967 when he was 16. Besides being CEO of the NAB, Argus had in 1996 joined the board of BHP Limited, one of largest mining companies in the world.

In 1999 Argus resigned as CEO and a director of NAB to become chairman of BHP. BHP merged in 2001 to become BHP Billiton Plc, the world's largest

Date	Events
1858	Founded in Melbourne as the National Bank of Australasia
1918	Colonial Bank of Australia (Est. 1855) acquired
1922	Bank of Queensland (Est. 1886) acquired
1948	Queensland National Bank (Est. 1842) acquired
1955	Ballarat Banking Company (Est. 1865) acquired
1981	Merged with the Commercial Banking Company of Sydney (Est. 1834) that had previously acquired the Bank of Victoria (Est. 1853)
1987	Clydesdale Bank (Est. 1838) acquired in Scotland
	Northern Bank (Est. 1824) acquired in Northern Ireland
	National Irish Bank (Est. 1996) acquired in the Republic of Ireland
1989	Don Argus joins board as an executive director with 41 years of banking experience
1990	Yorkshire Bank (Est. 1859) acquired in England
1992	Charles Allen joins board (forced to resign as chair in 2003)
	Don Argus appointed CEO
1992	Bank of New Zealand (Est. 1861) acquired
1995	Michigan National Corporation (Est. 1961) acquired in United States, sold in 2001 to offset losses
	Cathy Walter joins board of 13 as youngest (age 43) first-ever woman and only lawyer. She agrees to resign in 2004 to initiate a program of board replacement/renewal.
1996	CEO Don Argus joins board of BHP Limited as nonexecutive director
1997	Graham Kraehe joins board of 11. Charles Allen becomes chairman until forced to resign in January 2004; replaced by Kraehe, who agrees to resign in September 2005
	Cathy Walter appointed to Audit Committee with John MacFarlane as chair and other members Charles Allen, Dr. Christopher Deeley, and Mark Rayner
	Regulation of Australian banks removed from the Reserve Bank of Australia (RBA) to the newly formed Australian Prudential Regulatory Authority (APRA)
	Board approves purchase of U.S.-based HomeSide Inc. for $US1.2 billion (sold in 2001 after $A3.6 billion loss for which nobody is held accountable)
1998	Frank Cicutto, employed by the bank since 1967, joins board of 11 as an executive director, resigns as CEO in 2004 as a result of 2004 FX fraud and loss
1999	Don Argus resigns as CEO to become chair of BHP Billiton
2000	Cathy Walter appointed chair of Audit Committee with the two other most senior board members, Charles Allen and Mark Raynor, as its members
2001	**$A3.6 billion loss after tax from HomeSide operations and business put up for sale**
April	Michigan National Corporation Inc. sold for $A2.8 billion profit to offset loss
	Former KPMG audit partner Chris Lewis, who carried out the due diligence work on HomeSide acquisition, appointed General Manager, Group Risk Management (resigns on publication of APRA report into FX fraud/losses in March 2004)
Sept.	Mark Rayner forced to resign as chairman and a director as he is also chairman of the world's biggest zinc producer, Pasminco Limited, which went bankrupt from FX losses with $150 million owing to the bank
	Charles Allen becomes chairman; resigns when NAB FX fraud/losses are revealed in 2004
	FX losses hidden by smoothing spot FX trades
	Net profit decreased 35.7 percentage for group
	External auditor KPMG raises concerns over FX controls in its management letter
2002	APRA on-site review raises concerns only about IT systems
Feb.	PwC partner Jim Power contracted as internal auditor from February to August
May	Audit Committee chaired by Cathy Walter asks Jim Power if there are lessons from the FX trading fraud announced in Allied Irish Bank and is advised that there are not
	Board Audit Committee charter revised May; Graham Kraehe becomes a member
Aug.	Board considers establishing a subcommittee to review compliance and risk
Oct.	External auditor KPMG raises FX controls in its management letter

EXHIBIT 73.1 MILESTONES OF NATIONAL AUSTRALIA BANK LIMITED

Date	Events
Nov.	Management does not share APRA letter of concern dated November 21 with directors
2003 Jan.	APRA writes to bank chairman and executives on concerns over risk management, but Chairman Allen does not share the letter with the board
May	Cathy Walter as chair of Audit Committee requests copy of the letter tabled in May, but covering management letter by Chris Lewis downplays concerns
July	**Loss masking by surrendered spot FX trades begins**
	Risk Management Executive Committee downplays or ignores warnings
Aug.	John Stewart appointed as executive director; becomes CEO in 2004.
	APRA undertakes on-site review (Sarbanes-Oxley legislation becomes relevant)
Sept.	Audit Committee charter revised
Oct.	John Thorn, a former national managing partner the previous month of PwC and a member of its Global Audit Management Group, is appointed director and member of Audit Committee; he meets the Sarbanes-Oxley test of being a financial expert
	Fictitious options trades commence to conceal losses
Nov.	First Board Risk Committee established in August with Kraehe as chair
2004 Jan.	**FX losses of $A180 million announced January 13; FX losses revised on January 19 to $A185 million and revised again as being $A360 million January 27**
	PwC appointed by board to undertake investigation into FX losses; Cathy Walter raises concerns about PwC conflicts and suggests PwC could be sued, with PwC reported to counter with threat to take defamation action
	Deloitte Touche Tohmatsu retained to review whether the PwC report fairly and completely described and assessed the areas in which PwC faced a conflict of interest.
	Blake Dawson Waldron (BDW) solicitors retained as NAB's probity and governance advisors in respect of the PwC investigation (former chair of corporate regulator Australian Investment and Securities Commission is a consultant to BDW)
Feb.	Charles Allen resigns as chairman and nonexecutive director and Frank Cicutto resigns as CEO; Graham Kraehe is appointed chairman rather than Walter, who is the most senior nonexecutive director, with John Stewart as CEO and director
March	PwC report made public March 12. Chris Lewis, former KPMG audit partner, resigns as Executive General Manager—Risk Management
	John Thorn replaces Cathy Walter as chair of Audit Committee
	Seven nonexecutive directors give notice on March 21 of calling an extraordinary general meeting (EGM) on May 21 to remove Walter as a director; Walter gives notice on March 28, calling two separate EGMs on May 21 to remove all nonexecutive directors over time, censure the board, and limit their retirement benefits
	APRA report made public March 24 that uses information provided by PwC
May	Compromise established between Walter and board to cancel their EGMs with program for board renewal including Chairman Kraehe in September 2005; Walter resigns as a director in May and Malcolm Williamson is appointed a director
July	Audit Committee announces changes of auditor from KPMG to Ernst & Young for 2004 year
Aug.	Resignation of directors Kenneth Moss, Edward Tweddell, and Brian Clark
Sept.	Four new directors appointed, Paul Rizzo, Robert Elstone, Daniel Gilbert, and Jillian Segal, a former deputy chair of the corporate regulator, Australian Securities Investment Commission (ASIC)
Oct.	Two executives join the board, GM Australia, Ahmed Fahour, CFO, Michael Ullmer
Dec.	AGM with Michael Chaney appointed a director and chairman-elect in 2005

Source: Information obtained from NAB annual reports posted at http://www.nabgroup.com/0,,32863,00.html, NAB Company Secretary and APRA (2004). Media Reports for previous five years, except those for the period of Board turmoil from January to April 2004 are available at http://national.com.au/About_Us/0,,24173,00.html?ncID=ZBA

EXHIBIT 73.1 (*continued*) MILESTONES OF NATIONAL AUSTRALIA BANK LIMITED

diversified mining company. Another BHP nonexecutive director appointed in 1995 was Michael Chaney. Chaney joined the NAB board in December 2004 as chairman-elect for September 2005 to complete a board renewal program instigated by Walter. These events are included in Exhibit 73.1, which lists the milestones in the history of the bank with relevant events of "men behaving badly in banking."

73.3 EMERGING PROBLEMS

In 2001 the NAB reported an after-tax loss of $A3.6 billion from its HomeSide operations. It was the largest loss reported in Australian corporate history up to that time. To offset the loss, the U.S.-based Michigan National Corporation (acquired in 1995) was sold at a profit. The result was a 35.7 percent decline in reported net profit for the whole group.

The bank culture of no one being held accountable for errors was very publicly established, and no one was held accountable for the loss. Instead, Chris Lewis, who was the KPMG partner who had undertaken the due diligence on HomeSide before its purchase four years earlier, was hired by the bank to join the senior executive team as executive general manager—risk management.

The NAB chairman, Mark Raynor, was also chairman of Pasiminco Limited, the world's largest zinc producer and a customer of the bank. Pasiminco became bankrupt from unexpected FX losses in 2000. This forced Raynor to resign from the NAB board. Charles Allen as the next most senior director in terms of board tenure was appointed chairman. Walter became the second most senior nonexecutive director in terms of board tenure and so had a claim to be next in line to become chair of the bank.

It was also in 2000 that FX losses in the NAB were being hidden. This was through a process described as smoothing of spot FX trades (APRA 2004, 15). The loss of the chairman should have alerted all the NAB directors and staff of the dangers of FX trading.

The external auditor, KPMG, raised concerns about managing FX trading risks in its management letter of 2001. APRA made a site visit to NAB in 2001 but only raised concerns about the integrity of the information technology (IT) systems.

As NAB is an authorized deposit-taking institution, KPMG is required to present audit reports to APRA as the banking regulator. APRA (2004) made no mention of whether the KPMG 2001 statutory report on the NAB included concerns about operations of the foreign currency desk and market risk unit.

It would appear that APRA was asleep at the wheel like the directors. Auditors are not required, and in practice do not volunteer, to make public the concerns they raise in their annual management letter. The concerns they raise assist auditors to reduce their liability in any subsequent litigation on not discovering and reporting problems. It also provides a basis to sell consulting work to correct any problems that they identify. A diligent director or regulator would

requisition the annual management letter from the external auditor if not provided by management.

The need to requisition the management letter of auditors was included in the first course in the world to provide company directors with a professional qualification. The course, established in Australia in 1975, was suggested by the author in 1971 before the term *corporate governance* had come into vogue. I became a founding author of the course's four modules on "wider aspects of company direction," which warned directors to be concerned when the same points are raised by the auditors repeatedly in subsequent years. This would indicate that management is complacent and/or does not wish to change things. It also means that board colleagues and the regulator are not supervising and directing management adequately and/or have not bothered to read the auditors' management letter.

A similar conclusion was reached by APRA when they did review the audit management letters for their 2004 report, which stated on page 49:

> In reviewing the KPMG management letters for previous audits, APRA noted that a few issues had been outstanding for extended periods of time. As is the case for Internal Audit, APRA stresses that the closure of all issues is a vital process to ensure that control and procedures are in place to prevent both financial and reputational loss to the bank.

One might infer from this statement that the regulator had not earlier reviewed the management letters.

For six months from February to August 2002, Jim Power, a partner of PwC, was seconded to the NAB to head up its internal audit function. APRA (2004, 64) reported that "it appears that the regular scheduled meetings between the company and their external audit counterpart did not take place." During this time the charter of the Audit Committee was changed.

In February 2002 the Allied Irish Bank announced that it had suffered losses in its U.S. unit from fraudulent FX trading. Walter, as chair of the Audit Committee, requested Power to report if there were any lessons for the NAB. Power presented in person a memorandum that there were no issues of concern for the NAB in May 2002 (APRA 2004, 59). This might explain why Walter wanted to sue PwC when the FX fraud and losses were exposed in January 2004.

While "some concerns about traded market risk (including limit excesses)" came to the attention of the Audit Committee, these "were dampened by management" (APRA 2004, 54). APRA reported a conflict of interest in the management structure of the NAB. This arose from line executives being responsible for both profit and managing risk. A theme of the APRA report was that the NAB culture was one of not asking questions if profits were being obtained.

As the NAB had its shares traded in the United States, it was subject to the Sarbanes-Oxley Act (SOX), made law in July 2002. Compliance with SOX was required in 2003. The NAB board considered the need in 2002 to set up

a board subcommittee to review compliance and risk. There was also a need to have a director who met the test of being a being a "financial expert" as required by SOX. No NAB director was so qualified. In 2002, KPMG again raised in its annual management letter its concern over the FX trading.

In January 2003 APRA wrote to the bank with copies to both the chairman and management about "a lax approach to limit management; a culture of poor adherence to risk management policies;" and other concerns. However, this letter, like previous letters from APRA about its review in 2002, was not presented to the board or its committees (APRA 2004, 74). The Audit Committee only heard about the letters because of the concern expressed by Chris Lewis at their March 2003 meeting that the APRA letters had been circulated to Financial Service Authority in the UK. CEO Frank Cicutto agreed to bring up this concern at his next meeting with APRA (2004, 61).

This indicates how management did not take APRA seriously and why they did not share the substance of the letters with their directors. It also indicates how dependent nonexecutive directors are upon the information provided by management, to illustrate the fundament flaw of current practices. A process should be provided for directors to obtain information on a systemic basis independently of management.

Walter requested that the APRA letters mentioned by management at the March meeting be presented to their next meeting in May 2003. However, at the May meeting it appeared that only the covering memorandum prepared by management was read. According to APRA (2004, 61), "it did not reflect the gravity of the issues raised." A second letter from APRA of November 4 and the reply from Chris Lewis were also not raised for review by the Audit Committee (APRA 2004, 62).

In July 2003, APRA (2004, 16) reported that the fraudulent losses were being hidden by using surrendered spot FX trades.

In August 2003 the bank established a board risk management subcommittee chaired by Kraehe, who then relinquished his membership in the Audit Committee in September. In October 2003 John Thorn, who had been Australian managing partner and member of the PwC Global Audit Management Group the previous month, was appointed to the board to be the only director who met the test of being a financial expert pursuant to the Sarbanes-Oxley Act.

The Risk Management Committee's charter was approved in October and it had its first meeting on November 21 (APRA 2004, 63). It was at this time that fictitious option trades commenced to hide FX losses (APRA 2004, 16).

73.4 RENEWAL INTRODUCED BY TWO WHISTLE-BLOWERS

In January 2004 a junior employee blew the whistle on the cover-up of FX trading losses that amounted to $A360 million. As the only lawyer on the board, Walter thought there was a case for suing PwC for the losses. This could have exposed Thorn to personal liability as a former PwC partner. The press reported that PwC

was considering suing Walter for defamation over her concerns about the advice provided by PwC.

In February the chairman, Charles Allen, and the CEO, Frank Cicutto, resigned. The G7 protected PwC by appointing Kraehe as bank chair rather than Walter, who was then the longest-serving director. In addition, John Thorn was appointed to replace Walter as chair of the Audit Committee. There was now little possibility of PwC being exposed to criticism over its role as internal auditor and adviser. In addition, PwC was then commissioned by the board to investigate the cause of FX losses! APRA then used the PwC report to inform its official report.

However, in recognition of the conflict created by using PwC, the board also appointed a law firm, BDW, to advise on the probity of the process. In addition, they engaged another audit firm, Deloitte, to undertake part of the work where PwC had a conflict! Even to external observers these arrangements appeared a complex, contrived, and awkward way to proceed. Walter objected to how this process was implemented and would not undertake to remain silent.

When she refused the G7 request to resign to preserve board solidarity, the G7 acted very badly. Instead of waiting until the next annual meeting of shareholders and without sounding out lead institutional shareholders, they instigated a multimillion-dollar cost by calling an extraordinary general meeting (EGM) to remove Walter from the board.

The G7 justified their self-indulgent action with the 45,530 shareholders on the basis that they had "lost trust and confidence in Ms. Walter because of her misconceived criticism of the procedural integrity of the PwC report." Many shareholders were offended by their statement that "If Ms. Walter is not removed from the Board we have unanimously agreed that we would all resign from the Board as soon as practical." This was seen as blackmail to force a vote for the G7.

Walter then demonstrated the power of what a really independent director can achieve. She called additional EGMs for the staged retirement of all directors as their staggered three-year terms expired but with a resolution for her to be removed within seven days of the meeting. This eliminated the possibility of her being seen to act for her own self-interest and so contrary to Section 182(1)(a) of ACL, a view reinforced by her additional resolutions to censure the board and ask the directors to forgo their retirement allowances.

Australian corporate constitutions make legal unethical behavior of directors in chairing shareholder meetings at which they are being held accountable. In addition, directors are allowed to vote undirected proxy votes according to their personal interests and control the counting of votes that determine their appointment and remuneration (Turnbull 2002a)! The NAB chairman, Kraehe, resisted shareholder requests for a person not beholden to the directors to chair the EGMs. However, when Kraehe accepted shareholder demands in the media for his early retirement, a compromise process to renew the board was established with Walter resigning to allow the EGMs to be called off.

Walter had made her point and demonstrated what a single director can achieve when outvoted in the boardroom. Some people argue that resigning from a company and allowing a problem to be covered up makes the director an accomplice. Others state that directors should be made to state their reasons for resigning. However, such statements could expose them to Section 183(1)(b) of ACL pertaining to using information that they obtained as a director "to cause detriment of the corporation."

It was clear to everyone that Walter resigned to avoid further damage to the reputation of the bank from proceeding with the EGMs. It was not just because of her role as a director during the HomeSide and FX losses, as Kraehe was also a director at the time. The mutual ties of loyalty created by a staged renewal of the board is likely to inhibit any new directors from reviewing the role of PwC or whether the G7 contravened ACL Section 182(1)(b).

The events also raise questions about cronyism and misplaced loyalties that arise when audit partners transfer to client corporations. This also occurred with the 2001 collapse of an Australian insurance company, HIH, with losses of over $A5 billion, which was also subjected to APRA regulation. It cost the government over a billion dollars in underwriting the insurance contracts of thousands of businesses and employee entitlements.

In 2002 the NAB had proudly reported that it had been ranked first in a corporate governance survey of 250 of the largest Australian listed companies. The survey stated, "Corporate governance structures were outstanding. The structures met all the best practice standards and could not be faulted." This illustrates the irrelevance of so called best practices and so also the provisions of the Sarbanes-Oxley Act. APRA (2004, 5) reported that "NAB's internal control systems failed at every level to detect and shut down the irregular currency options trading activity."

The APRA report repeatedly noted how management had failed to share information with the directors and/or had hidden its importance. It documented how difficult it is for directors to know what questions to ask and when their trust in management might be misplaced.

One of the most important fundamental functions of directors is to monitor management. It makes no sense for this to be undertaken by relying *only* on reports provided by management. Indeed, it could be considered irresponsible and a dereliction of the duty to exercise due care and vigilance as required by Section 180 of ACL.

Courts of law do not generally rely on the evidence *only* provided by the accused without independent collaboration. But directors of U.S., UK, and Australian publicly traded companies lack a systemic process to validate the information provided to them by management or the integrity of the messenger and the messenger's messenger.

73.5 WHY BEST PRACTICES CANNOT PREVENT PROBLEMS

There are two inconvenient truths about all Anglo-type publicly traded companies:

1. Directors have no systemic processes for carrying out their most fundamental roles with information obtained independently of management to direct and monitor management or learn when their trust in management is misplaced.
2. Directors have absolute power to manage their own conflicts of interest that can corrupt absolutely both themselves and the organization.

Systemic solutions to these problems are described in the public policy booklet on *A New Way to Govern: Organizations and Society after Enron* (Turnbull 2002b) and in a number of related articles (Turnbull 2000, 2002a, 2006).

To obtain information independently of management, directors need feedforward and feedback information from separate advisory forums for each stakeholder group of record established by the corporate constitution to be independent of the grace and favor of management (Turnbull 2000, 2006). Likewise, corporate constitutions need to introduce a more appropriate division of powers between shareholders and directors by establishing what Australian Senator Andrew Murray (1998) described as a "corporate governance board" (CGB). The concept of a CGB was based on a corporate senate (Turnbull 2002a) established by an Australian start-up company to attract additional equity investment from its U.S. shareholders. Both a CGB and a corporate senate create a process to mediate board conflicts of interest and disputes privately and in a way to protect shareholders' interests and the reputation of the firm.

Corporate law, regulations, listing rules, and governance codes are typically based on practices. However, what are more important to directors, investors, and stakeholders are outcomes. An outcome-based approach would allow competition among firms to find the most efficient and effective practices to protect and further the interest of the company and its stakeholders (Turnbull 2007). This is inhibited or prevented by the current approach based on practices. An outcome-based approach would also introduce systemic solutions.

Some practices have little or no empirical evidence or an analytical basis to support their effectiveness. The ever more complex practices and definitions associated with trying to define the independence of auditors or directors is a case in point. As the purpose of an external audit is to check the report of independent and nonindependent directors alike, it is impossible for auditors to be independent in the ordinary meaning of the word when they are engaged by the directors. No court of law would describe a judge as independent if she was judging someone who engaged and paid her. If the outcome sought is to protect investors from fraud, then a much more effective way would be to remove the need for corporations to appoint an auditor if they obtained insurance on the accuracy of their

financial statements. It would then be the insurance company that would appoint what would then become an "investigating accountant" as used by bankers to report on the integrity of a business to repay their loans (Turnbull 2005).

Likewise, there are different outcomes that could be achieved in a much more efficient and effective manner than relying on directors to meet some test of independence. Instead of relying on directors, watchdog boards could be formed by amending the corporate constitutions to provide some of the outcomes expected from appointing independent directors. The watchdog boards could also be used to mediate conflicts of interest (Turnbull 2002b, 2005). Stakeholder forums can achieve other outcomes that independent directors might be expected to perform (Turnbull 2006).

The most compelling reason for adopting an outcome-based approach is that it can be grounded in the science of corporate governance (Turnbull 2002c). It provides a rational and rigorous basis for simplifying laws, regulations, and listing rules to eliminate the need for corporate governance codes. It is because the law, regulators, and listing rules fail to produce satisfactory outcomes that corporate governance codes are required.

An outcome-based regulatory strategy depends on stakeholders (whom the law and listing rules are designed to protect) becoming involved as co-regulators. A strategy for introducing deregulation through self-enforcing co-regulation is described in Turnbull (2006, 2007).

There are a number of take-home messages from "men behaving badly in banking." These are:

1. The inherent conflict of interest of directors relying on management to monitor and direct the business
2. The inherent conflict of interest of directors evaluating management by the information only provided by management
3. The inherent conflict of interest of regulators relying on information provided by those subjected to their regulation such as directors, management, and auditors
4. The conflict of interest for auditors blowing the whistle on those who engage them
5. The impotence of a single director to make a difference privately
6. The absence of any internal system for conflict resolution within boards
7. The need for individual directors to use extreme action to protect a company and/or themselves, like calling an EGM that would not be available in many other jurisdictions
8. The impotence of best practices in corporate governance to either avoid the aforementioned problems or to enhance performance
9. The need for basing regulation on outcomes rather than practices to simplify the law

10. The need for *A New Way to Govern* that introduces self-regulation through self-enforcing processes as described earlier by introducing stakeholders (whom the law seeks to protect) as co-regulators (Turnbull 2007)

Note: The career of Cathy Walter as a professional nonexecutive director survived her experience at the NAB. In 2006 at the age of 54 she was a nonexecutive director of three of the top 100 listed companies in Australia: Australian Foundation Investment Company Limited, the largest listed Australian investment company; Australian Stock Exchange Limited; and Orica Limited. She was a director of the Melbourne Business School Limited, member of the Financial Reporting Council, and chair of the federal government's Business Regulation Advisory Group.

References

ACL. 2001. *Corporations Act 2001*. Australian Corporate Law. Available at http://scaletext.law.gov.au/html/pasteact/3/3448/top.htm.

APRA. 2004. *Report into irregular currency options trading at the National Australia Bank*. Sydney: Australian Prudential and Regulatory Authority, March 23. Available at www.nabgroup.com/vgnmedia/downld/APRAreport_24march04.pdf.

Murray, A. 1998. *Minority report: Report on the company law review bill, 1997.* Parliamentary Joint Committee on Corporations and Securities, March, Parliament of the Commonwealth of Australia. Available at www.aph.gov.au/senate/committee/corp_sec_ctte/companylaw/minreport.htm.

Turnbull, S. 2000. Corporate charters with competitive advantages. *St. Johns Law Review* 74 (44) (Winter): 101–59. Available at http://ssrn.com/abstract=10570.

Turnbull, S. 2001. Why regulation of financial institutions cannot be assured with a unitary board. Presented to 14th Australasian Finance and Banking Conference, December 18, Sydney. Available at http://papers.ssrn.com/paper.taf?abstract_id=310501.

Turnbull, S. 2002a. Corporate watchdogs: Past, present and future. Available at http://papers.ssrn.com/abstract_id=608244.

Turnbull, S. 2002b. *A new way to govern: Organizations and society after Enron*. London: New Economics Foundation. Available at http://ssrn.com/abstract_id=319867.

Turnbull, S. 2002c. The science of corporate governance. *Corporate Governance: An International Review* 10 (4) (October): 256–272. Available at http://ssrn.com/abstract_id=316939.

Turnbull, S. 2003. A new way to govern: Because "world best practices" are the problem not the solution. Presented to Chartered Secretaries Australia 2nd Annual Corporate Governance Symposium, March 4, Sydney. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=386740.

Turnbull, S. 2004. Why Anglo corporations should not be trusted: And how they could be trusted. *FER Forum*, Financiële Studievereniging, Erasmus University, Rotterdam, 6 (2) (February): 6, 7, 9–15. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=492524.

Turnbull, S. 2005. How US and UK auditing practices became muddled to muddle corporate governance principles. *ICFAI Journal of Audit Practice* 2 (3) (July): 49 − 68. Available at http://ssrn.com/abstract=608241.

Turnbull, S. 2006. Enhancing organizational performance and social responsibility with self-regulation. Presented to the Society for the Advancement of Socio-economics, University of Trier, Germany, July 1, and to the International Corporate Governance Conference, University of Birmingham Business School, July 3. Available at http://ssrn.com/abstract=906441.

Turnbull, S. 2007. Streamlining regulation with self-enforcing co-regulation. Submission to the Australian Treasury of February 14th in response to its Streamlining Prudential Regulation Project. Available at http://papers.ssrn.com/abstract_id=979531.