2nd Edition

FINANCIAL STATEMENT FRAUD

PREVENTION and DETECTION

Zabihollah Rezaee   Richard Riley

FINANCIAL STATEMENT FRAUD

Prevention and Detection

Second Edition

ZABIHOLLAH REZAEE
RICHARD RILEY

WILEY

John Wiley & Sons, Inc.

Copyright © 2010 by John Wiley & Sons, Inc. All rights reserved.

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

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, 201-748-6011, fax 201-748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

For more information about Wiley products, visit our Web site at http://*www.wiley.com*.

Library of Congress Cataloging-in-Publication Data:
Rezaee, Zabihollah, 1953-
Financial statement fraud : prevention and detection / Zabihollah Rezaee, Richard Riley. – 2nd ed.
p. cm.
Includes index.
Summary: ‘‘Practical examples, sample reports, best practices and recommendations to help you deter, detect, and prevent financial statement fraud Financial statement fraud (FSF) continues to be a major challenge for organizations worldwide. Financial Statement Fraud: Prevention and Detection, Second Edition is a superior reference providing you with an up-to-date understanding of financial statement fraud, including its deterrence, prevention, and early detection. You will find A clear description of roles and responsibilities of all those involved in corporate governance and the financial reporting process to improve the quality, reliability and transparency of financial information. Sample reports, examples, and documents that promote a real-world understanding of incentives, opportunities, and rationalizations Emerging corporate governance reforms in the post-SOX era, including provisions of the SOX Act, global regulations and best practices, ethical considerations, and corporate governance principles Practical examples and real-world ‘‘how did this happen’’ discussions that provide valuable insight for corporate directors and executives, auditors, managers, supervisory personnel and other professionals saddled with anti-fraud responsibilities Expert advice from the author of Corporate Governance and Ethics and coauthor of the forthcoming Wiley textbook, White Collar Crime, Fraud Examination and Financial Forensics Financial Statement Fraud, Second Edition contains recommendations from the SEC Advisory Committee to reduce the complexity of the financial reporting process and improving the quality of financial reports’’–Provided by publisher.
ISBN 978-0-470-45570-8
1. Misleading financial statements. 2. Fraud. I. Riley, Richard, 1962- II. Title.
HF5681.B2R3997 2010
657'.3–dc22 2009025053

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

This book is dedicated to Dr. Rezaee's son Nick and Dr. Riley's parents Dick Sr. and Betty, wife Shelley, and children Connor, Andrew, and Kelsey

Contents

Foreword **xi**

Preface **xiii**

Acknowledgments **xix**

Part One: Financial Reporting and Financial Statement Fraud **1**

1 Financial Statement Fraud Defined **3**

Will History Repeat Itself? 3
A Closer Look 4
Definition of Financial Statement Fraud 4
Nature of Financial Statement Fraud 8
High-Impact Fraud Cases 11
Cost of Financial Statement Fraud 13
Fraud Studies and Regulatory Responses 16
Antifraud Programs 19
Occurrence, Prevention, and Detection 22
Lessons Learned and Applications for Practice 25
Notes 28

2 Financial Reporting Structure **31**

Introduction 31
Financial Reporting System 31
Importance of Financial Information 33
Annual Financial Reporting Requirements 38
High-Quality Financial Reports 39
Six-Legged Stool of the Financial Reporting Process 41
Corporate Financial Reports 42
Corporate Reporting Challenges 44
Financial Restatements 45
Fair Value 46
Stock Options Accounting 46
XBRL-Generated Financial Reports 47
Antifraud Applications for Practice 48
Notes 52

Part Two: Financial Statement Fraud Profile, Taxonomy, and Schemes 55

3 Cooking the Books Equals Fraud 57

Introduction 57
Why Does Financial Statement Fraud Occur? 57
Profile of Financial Statement Fraud 58
Waste Management, Inc.: Financial Statement Fraud Analysis 70
Antifraud Applications for Practice 72
Notes 76

4 Realization, Prevention, and Detection 78

Introduction 78
Realization 78
The 3Cs Model 79
Financial Statement Fraud Prevention 84
Financial Statement Fraud Detection 86
Correction Procedures 87
Prevention, Detection, and Correction Strategies 87
Antifraud Applications for Practice 89
Notes 96

5 Taxonomy and Schemes 97

Introduction 97
Symptoms of Financial Statement Fraud 97
Common Fraud Schemes 101
Common Revenue Fraud Schemes 103
Financial Statement Fraud Red Flags 105
Whistle-blower Regulations 112
Antifraud Applications for Practice 114
Notes 117

Part Three: Corporate Governance and Its Role in Preventing and Detecting Financial Statement Fraud 119

6 Role of Corporate Governance 121

Introduction 121
Definition of Corporate Governance 122
Role of Corporate Governance 122

Corporate Governance Structure 125
Characteristics of Corporate Governance 127
Corporate Governance Functions 128
Global Corporate Governance 132
Antifraud Applications for Practice 134
Notes 136

7 Board of Directors' Oversight Responsibility 138

Introduction 138
Role of the Board of Directors 138
Composition of the Board of Directors 139
Functions of the Board of Directors 142
Attributes of Boards of Directors 145
Antifraud Applications for Practice 151
Protocol: A Plan for Reaction to Allegations of Misconduct 152
Notes 155

8 Audit Committees and Corporate Governance 157

Introduction 157
Audit Committee 157
Audit Committee Attributes 166
Audit Committee Roles and Responsibilities 168
Audit Committee Charters 172
Chairperson of Audit Committees 173
Audit Committee Report 173
Audit Committee Roles in Preventing and Detecting
Financial Statement Fraud 177
Antifraud Applications for Practice 178
Notes 183

9 Management Responsibility 184

Introduction 184
Management Financial Reporting Responsibilities 184
Management's Role in Financial Statement Fraud
Prevention and Protection 190
Management Motives and Incentives 191
Management Override of Internal Control 192
Gamesmanship 194
Risk Management 196
Antifraud Applications for Practice 200
Notes 204

10 Role of the Internal Auditor 206

Introduction 206
Internal Auditors and Corporate Governance 206
Internal Auditors' Responsibilities 208
Internal Audit Fraud Standards 212
Efficacy of Internal Audit in Financial Statement Fraud Prevention and Detection 214
Cooperation between External and Internal Audit 215
Internal Audits and the Audit Committee 217
Internal Control 218
Antifraud Applications for Practice 225
Notes 227

11 Role of External Auditors 229

Introduction 229
Independent Audit of Financial Statements 229
Independent Auditor and Financial Statement Fraud 234
Independent Audit and Internal Control 237
Report on Internal Controls 238
Fraud Detection Audit Procedures 240
Materiality Guidance 246
Risk Factors of Financial Statement Fraud 249
Communication of Fraud 253
Antifraud Applications for Practice 254
Notes 256

12 Governing Bodies 258

Introduction 258
Role of Regulation in Corporate Governance 259
Sarbanes-Oxley Act of 2002 260
Securities and Exchange Commission 263
SEC's Regulation Fair Disclosure 267
Financial Fraud Detection and Disclosure Act of 1992 268
Private Securities Reform Act of 1995 268
SEC and Financial Statement Fraud 269
SEC Fraud Prevention Activities 269
SEC Fraud Detection Activities 270
SEC Fraud Enforcement Activities 270
Role of the Financial Accounting Standards Board 273
Antifraud Applications for Practice 276
Notes 279

Part Four: Digital (Computer) Approaches to Fraud and Forensic Accounting 281

13 Fraud in a Digital Environment 283

Introduction 283
Digital Economy 284
Electronic Commerce 285
Changes in Business Environment 288
Electronic Financial Reporting 292
Antifraud Applications for Practice 302
Notes 305

14 Fraud Examination Practice, Education, and Research 306

Introduction 306
The Interrelationship: Auditing, Fraud Examination, and Forensic Accounting 307
Forensic Accounting Practice 308
Fraud Examination 310
Certification in Financial Forensics 313
Training Competent and Ethical Fraud Examiners and Forensic Accountants 313
Fraud Examination and Forensic Accounting Education 315
Role of Research in a Profession 316
Antifraud Applications for Practice 318
Notes 321

Appendix: Summary of Six Recent Fraud Studies 323

About the Authors 327

Index 329

Foreword

In this new century, financial statement fraud has increasingly become a serious problem for business, government, and investors. Indeed, the issue threatens to undermine the confidence of capital markets, corporate leaders, and even the venerable audit profession.

Auditors in particular have been hit hard for their seeming inability to find fraud on a massive scale. Monetary judgments in the hundreds of millions of dollars against certified public accounting (CPA) firms have become commonplace, and one of the largest auditing firms, Arthur Andersen, has completely disappeared.

Many who know say the audit process—as we have known it for generations—is doomed. But that may not be all bad. For if an audit fails to find these huge crimes, engineered at the very top of our public enterprises, what good is it?

The United States Supreme Court agreed with that premise in 1984 when it affirmed that the independent auditor was indeed the ‘‘public watchdog.’’ But in the quarter-century since that pronouncement, we’ve continued to see too many situations where the watchdog was asleep, toothless, or too old to chase its quarry.

To learn history’s valuable lessons, we need to look at where we’ve been in order to know where we should be going. From recorded history until the beginning of the 1900s, the auditor’s primary role was to detect and deter fraud. It was much easier to do back then: Businesses were small, financial transactions were fewer, and transnational corporations and financial conglomerates were unheard of.

But as commerce picked up speed, the auditor had to do more with less; scrutinizing each and every transaction for fraud became a physical impossibility. From the time of the stock market crash of 1929—due in no small part to rampant fraud—until the 1980s, the focus of the audit became different. During that period, the auditor spent most of his effort on reporting issues.

It didn’t take financial scoundrels long to notice that the watchdog wasn’t barking any more. In the 1970s, an enterprising insurance salesman named Stanley Goldblum made a mockery of the audit as it had been traditionally conducted. Right under the nose of his independent CPA firm, Goldblum’s company, Equity Funding, easily managed to add 65,000 phony policyholders to its rolls, along with $800 million in fake assets.

Goldblum’s scam was only the beginning of a cascade of spectacular audit failures, from the savings and loan debacle to Enron, WorldCom, and Madoff. And the refrain has only grown louder: ‘‘Where were the auditors?’’

The answer, strangely enough, is that the auditors were too busy auditing to find fraud. But don’t blame them, for they were doing only what they were taught. Or, more correctly, *not* taught.

As any accounting graduate in the last 30 years will tell you, the amount of antifraud training in college is not just inadequate; it has been practically

nonexistent. Part of the reason has been the lack of authoritative texts in the field. Luckily, with books like this one, that is changing.

Zabihollah Rezaee and Richard Riley's second edition of *Financial Statement Fraud: Prevention and Detection* is bound to make a real difference. Exceptionally well researched and chocked with up-to-date case examples, *Financial Statement Fraud* not only explains in understandable language how these schemes are committed, it offers valuable advice on how to prevent and detect them.

But the authors' work goes much beyond helping educate accounting students and auditors. It is a valuable reference guide for fraud examiners, audit committees, management, and regulators; and one other important cog in this wheel: the investors who stand to lose everything.

Education is the sword needed to strike a blow against white-collar crime. And in this war, *Financial Statement Fraud* can be a powerful weapon.

Joseph T. Wells, CPA, CFE
Founder and Chairman
Association of Certified Fraud Examiners

Preface

Trust is the bedrock of the financial markets. Financial statement fraud *violates that trust.* This book empowers readers by articulating best practices in financial statement fraud prevention, deterrence, detection, and investigation. It accomplishes that goal by thoroughly examining some of the ''how it was done'' of the most notorious frauds of the last 25 years—Enron, WorldCom, Adelphia, Bernard Madoff, Stanford Financial, Satyam, and even Al Capone—by carefully examining the roles and responsibilities of the major players in the corporate governance fabric—the board of directors, audit committees, senior management, internal auditors, external auditors, and regulators—and by describing best practice tools and techniques that will help readers identify, investigate, and remediate fraud in their own organizations.

As evidenced by the catastrophic collapse of the real estate market and the financial industry's meltdown in 2008, efficiency, liquidity, safety, and robustness of financial markets are vital to the nation's economic prosperity and growth, as more than 110 million Americans directly or indirectly invest in the capital markets. Investors invest as long as they have confidence in the quality, reliability, and transparency of the financial information, including audited financial statements. Financial statement fraud is a serious threat to the market participants' confidence in financial information. The existence and persistence of financial fraud continues to be of great concern for regulators and the business and investment community. In short, the ''fraud problem'' is ever persistent and growing. Since July 2002, the Department of Justice has obtained nearly 1,300 fraud convictions. That's right; some 1,300 fraudsters are now in jail. But the tragedy goes beyond those found culpable: employees lose jobs, investors' 401(k)s are wiped out, and wealth disappears overnight. This book provides insight into how readers can help to prevent, deter, and detect fraud as early as possible.

The recent economic downturn provides incentives and opportunities for management to engage in financial statement fraud. Management is under a greater pressure to manage earnings and cooking the books is a way to achieve financial targets to meet investors' and analysts' expectations of sustained performance. Also, the opportunities to engage in financial statement fraud are higher during economic downturns, as many companies seek to reduce costs and compromise investment efforts in internal controls, governance mechanisms, and risk management. And when the ''river level drops, more rocks appear''; similarly, during difficult financial times, more frauds become apparent. During financial crises and economic meltdowns, the focus on financial statement fraud prevention and detection is more important than ever, as investors, regulators, and companies seek a better understanding of corporate malfeasance and misconduct. During the recent financial turmoil in capital markets, the Securities and Exchange Commission

(SEC) has taken several actions to combat fraud and security law violations, including initiating more than 50 pending investigations in the subprime area, charging managers of hedge funds for fraudulently misleading investors, charging brokers for defrauding customers, and examining Fannie Mae and Freddie Mac for accounting fraud. Likewise, the Federal Bureau of Investigation is experiencing an exponential rise in fraud cases, recently reporting more than 2,000 investigations regarding mortgage fraud and 566 corporate-fraud investigations.

So how does this happen? Financial fraud perpetrators are generally model citizens prior to their downfall—they are important members of the community, well-educated, often married with children and even grandchildren, exceptionally successful—and the list goes on. Boards of directors, audit committees, senior management, and regular employees should recognize that one incident of financial statement fraud can severely damage many years of investor confidence in their company's integrity. Effective corporate governance, a functioning system of checks and balances, a reinforced code of conduct, effective antifraud programs, a whistle-bower hotline, whistle-blower protections, and similar procedures can prevent, detect, and mitigate fraud. Further, the risk of collusive behavior and management override can be significantly reduced when there is an effective code of conduct, risk management, governance oversight, and whistle-blower functions.

While rules and regulations reduce incentives and opportunities for perpetrators to commit fraud, strong corporate governance and antifraud education and practice, including employee and public awareness and investor vigilance, are often most effective in preventing and detecting financial statement fraud.

The study of financial statement fraud and a book such as this are valuable primarily because the efficiency and health of companies, as well as the greater capital markets, largely depends on the quality, integrity, usefulness, and reliability of financial information. The prevention and detection of financial statement fraud are crucial to the economic growth and prosperity of the United States. This book also assesses the consequences of financial statement fraud and its impact on people—real people—and on the integrity and quality of the financial reporting process. Additionally, it suggests ways to improve prevention, deterrence, and detection. Generally, the overwhelming majority of publicly traded companies in the United States have responsible governance, use a reliable financial reporting process, and conduct their business in an ethical and legal manner; however, because ''one bad apple spoils the barrel,'' the entire society, business community, accounting profession, and government have a vested interest in preventing and detecting financial statement fraud so as not to undermine the confidence in corporate America.

PURPOSE OF THE BOOK

High-profile cases of financial statement fraud such as HealthSouth, Phar-Mor, Tyco, ZZZZ Best, and others have raised serious concerns regarding a lack of adequate and responsible corporate governance and accountability. Fraud is everyone's

responsibility. Nevertheless, it is the top management team's responsibility to prevent it before it occurs and to design adequate and effective internal control structures to detect and correct fraudulent activities. The ''tone at the top'' set by corporate leadership, including the board of directors and its representative audit committees, to disallow any unusual business practices, aggressive accounting methods, earnings management, or violations of the company's applicable laws and regulations, as well as code of business conduct, plays an important role in preventing and detecting financial statement fraud. By focusing on the role of governance, this book provides all stakeholders, including managers, supervisors, and employees, with a better understanding of why financial statement fraud occurs and how it can be prevented and detected. This book underscores the significance of, and provides theoretical and practical guidance to recognize, prevent, detect, and correct, financial statement fraud. The contents of this book, including a brief synopsis of each chapter, are summarized to provide the reader with an overview of the upcoming themes.

As this book was going through the production process in 2009, the 111th Congress introduced several bills designed to combat white-collar crime, particularly financial statements fraud in financial institutions. These bills were introduced in response to recent financial crises and the resulting global economic meltdown and to address fraud issues in several areas, including (1) financial market fraud (the supplement Anti-Fraud Enforcement Markets Act, the Fraud Enforcement and Recovery Act), (2) mortgage lending fraud (the National Mortgage Fraud Task Force Act, the Stop Mortgage Fraud Act, the Foreclosure Rescue Fraud Act), (3) Medicare fraud (the Medicare Fraud Prevention and Enforcement Act), and (4) government spending fraud (the Whistleblower Protection Enforcement Act) and tax fraud (the Stop Tax Haven Abuse Act).

Financial statement fraud continues to be a major challenge for organizations worldwide, and the persistence of it in the post–Sarbanes-Oxley (SOX) era reflects the severity of financial statement fraud and the recognition of the urgent need for antifraud practice and education.

Financial Statement Fraud: Prevention and Detection, second edition, is a superior reference for all business professionals who need an up-to-date understanding of financial statement fraud, including its deterrence, prevention, and detection. Unlike other fraud books that focus primarily on occupational fraud, the 300+ pages of *Financial Statement Fraud* provide a clear description of the roles and responsibilities of all those involved in the financial reporting process, including the board of directors, senior executives, internal and external auditors, legal counsel, financial advisors, employees, and investors in deterring, preventing, and detecting fraud. Straightforward language illustrates theoretical and practical concepts and procedures to aid comprehension of complex financial reporting processes and exposure to a variety of fraudulent activities. Sample reports, examples, and documents promote a real-world understanding of incentives, opportunities, and rationalizations for financial reporting participants to engage in financial statement fraud. This second edition incorporates emerging corporate governance reforms in the post-SOX era, including provisions of the SOX Act, global

regulations and best practices, ethical considerations, and corporate governance principles. The emerging issues of ethics and corporate governance are integrated into all chapters. The new edition also includes features, practical examples, and refinements valuable to professionals of all levels, corporate leaders, directors, executives, and educators, without compromising the book's practical utility for auditors and practitioners. Enhancements have been made to the content, style, clarity, and presentation of materials throughout the book.

This book is helpful to the following:

Auditors. Internal and external auditors should find the chapter materials relevant, useful, and suitable to their audit functions, gearing their audit procedures toward fraud prevention and detection.

Corporations, their board of directors, audit committees, executives, legal counsel, managers, supervisors, and employees. Best practices of corporate governance, financial reporting and audit functions, provisions of SOX and related SEC implementation rules, and Public Accounting Oversight Board (PCAOB) auditing standards discussed throughout the book should help public companies and their boards of directors, executives, and legal counsel effectively discharge their responsibilities in producing high-quality financial reports, free of material misstatements caused by errors and fraud.

Business schools and training programs. The book can also be used easily in educational and training programs of business schools and professional organizations. Other professionals, such as management accountants, internal auditors, corporate legal counsel, financial institutions, and financial analysts who provide accounting, auditing, legal, and financial services to corporations, should find this book relevant and helpful to their professional services and activities.

International practitioners and students. Discussions of global corporate governance and convergence in financial reporting and auditing standards make the book attractive to corporations, business schools, and professionals worldwide. Notable coverage includes discussion of corporate governance models throughout the world, international financial reporting standards (IFRS), and international auditing and assurance standards (IAAS).

HIGHLIGHTS OF THE SECOND EDITION

- Regulatory reforms and best practices in the post-SOX era are integrated into all 14 chapters.
- Each chapter includes chapter objectives and a summary.
- Practical examples, such as Enron, WorldCom, Adelphia, Tyco, HealthSouth, and others, and sample reports and documents, are incorporated into all chapters.

- Financial statement fraud cases incurred in the post-SOX period, including Madoff, Stanford Financial, and Satyam and their deterrence are presented throughout the text.
- All chapters have been updated to address emerging initiatives affecting financial reporting and corporate governance and auditing functions (SOX- and SEC-related implementation rules, auditing standards issued by the PCAOB, technological advances, and globalization).
- Recommendations from the SEC Advisory Committee to reduce the complexity of the financial reporting process and improve the quality of financial reports are woven all through.
- Recommendations from the Treasury Advisory Committee to improve audit quality are incorporated throughout.
- Integrated audit of financial statements and internal control over financial reporting, in compliance with PCAOB Auditing Standards No. 5 and its impact in reducing fraud, are added into related chapters.
- The emerging financial reporting and auditing initiatives, including the movement toward IFRS and IAAS, as well as the use of the XBRL reporting platform, are discussed.
- Antifraud programs, procedures, and trainings are integrated throughout.
- An entire chapter is dedicated to the role of technology in financial statement fraud.

ORGANIZATION OF THE BOOK

The focus of the second edition continues to be on the importance of corporate governance in preventing and detecting financial statement fraud, including examinations of real-world frauds and practical tools and techniques for carrying out their antifraud responsibilities. The organization of the second edition provides the maximum flexibility in choosing the amount and order of materials on financial statement fraud. This book is organized into four parts, as follows:

Part	Subject	Chapters
1	Financial Reporting and Financial Statement Fraud	1 & 2
2	Financial Statement Fraud Profile, Taxonomy, and Schemes	3–5
3	Corporate Governance and Its Role in Preventing and Detecting Financial Statement Fraud	6–12
4	Digital (Computer) Approaches to Fraud and Forensic Accounting	13 & 14

Each chapter starts with an examination of a real-world fraud as a basis for further examination of the chapter’s specific topics, and each chapter closes with a section titled “Anti-fraud Applications for Practice,” which helps the reader further

identify how to apply the chapter's material to preventing, detecting, and deterring fraud. The 14 chapters of the second edition are organized into four parts. Part I contains two chapters, which describe the importance of financial information in our capital markets and our society as well as the persistence of financial statement fraud that continues to threaten the integrity and quality of the financial reporting process even in the post–Sarbanes-Oxley Act. These chapters examine financial statement fraud, its definition, costs, and the nature and significance as well as the financial reporting process of publicly traded companies.

Part Two, presented in Chapters 3 through 5, discusses financial statement fraud profiles, taxonomies, and schemes as well as antifraud education, programs, and practices to prevent and detect them. Chapter 3 presents profiles of several companies alleged by the SEC for engaging in financial statement fraud, reviews their alleged financial statements fraud cases, and demonstrates that ''cooking the books'' causes financial statement fraud, which results in a crime. Chapter 4 presents a model consisting of conditions, corporate structure, and choices (the 3Cs) in explaining and analyzing motivations, opportunities, and rationalizations for the commission of financial statement frauds. Chapter 5 identifies and discusses taxonomies and schemes of financial statement fraud in an attempt to provide a better understanding of the symptoms (red flags) of financial statement fraud and management motivations to engage in financial statement fraud.

Part Three consists of Chapters 6 through 12, which constitute the foundation of the book. Chapter 6 defines corporate governance and its participants and roles in preventing and detecting financial statement fraud. Chapter 7 discusses the role of the board of directors in overseeing corporate governance and the financial reporting process. Chapter 8 examines the audit committee's role in overseeing the effectiveness of corporate governance, integrity, and quality of financial reports, adequacy and effectiveness of internal control structure, and quality of audit function. Chapter 9 discusses the role of management in corporate governance and the financial reporting process. Management is primarily responsible for the quality, integrity, and reliability of the financial reporting process. Chapter 10 examines internal auditors' responsibility for prevention and detection of financial statement fraud. Chapter 11 discusses the responsibility of independent auditors in discovering financial statement fraud and providing reasonable assurance regarding the quality, integrity, and reliability of published financial statements. Chapter 12 discusses the role of several governing bodies (e.g., SEC, FASB, AICPA, PCAOB, IASB, NYSE, NASD) that directly or indirectly influence corporate governance and the financial reporting process of publicly traded companies.

Part Four includes two chapters. Chapter 13, titled ''Fraud in a Digital Environment,'' examines electronic commerce strategies, changes in business environment, electronic financial reporting (including extensible business reporting language [XBRL]), and computer fraud. Chapter 14 presents forensic accounting practices, including fraud examination, litigation consulting engagements, and expert witnessing services. This chapter also discusses forensic accounting education and methods of integrating forensic accounting topics into the accounting curriculum.

Acknowledgments

We acknowledge the Public Company Accounting Oversight Board, American Institute of Certified Public Accountants, Institute of Internal Auditors, Institute of Management Accountants, Association of Certified Fraud Examiners, Securities and Exchange Commission, and Big Four Accounting Firms for permission to quote and reference their professional standards and other publications. We also recognize the quality reporting that is cited throughout the book, including the *Wall Street Journal*, *Washington Post*, *USA Today*, the *New York Times*, and others.

The encouragement and support of our colleagues at the University of Memphis and at West Virginia University are also acknowledged. The assistance of Dr. Rezaee's graduate student, Anna Anatolyevna Uboytseva, is also appreciated. We thank the members of the John Wiley & Sons, Inc., team for their hard work and dedication, including Chris Gage for managing the book through the production process, Andrew Wheeler for his marketing efforts, and Helen Cho, Tim Burgard, and John DeRemigis for their editorial guidance.

Our sincere thanks are due to our families, the Rezaee family, Soheila, Rose, and Nick; and the Riley family, Shelley, Connor, Andrew, and Kelsey. Without their love, enthusiasm, and support, this book would not have come to fruition when it did.

Zabihollah Rezaee
Richard Riley

Part One

Financial Reporting and Financial Statement Fraud

Chapter 1

Financial Statement Fraud Defined

WILL HISTORY REPEAT ITSELF?

The existence and persistence of financial fraud continues to be of great concern for regulators and the business as well as the investment community. Since July 2002, the Department of Justice (DoJ) has obtained nearly 1,300 fraud convictions. These figures include convictions of more than 200 chief executive officers (CEOs) and corporate presidents, more than 120 corporate vice presidents, and more than 50 chief financial officers[1] (CFOs). To combat this problem, the 2002 Sarbanes-Oxley Act (SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, was signed into law. Despite changes in regulation and oversight, a question remains: Are we destined to suffer through more of these types of nefarious acts? Or more simply, will history repeat itself? Ironically, the answer is yes, according to the 2008–2009 KPMG Integrity Survey, which suggests the prevalence of corporate fraud and malfeasance.[2]

Consider the following.[3]

Basis of the Fraud	Older Example	Year	Recent Example	Year
Fictitious revenue, documentation forgery, and theft of corporate assets	ZZZZ Best	1987	Enron	2001
Personal use of assets, false documentation, and financial statement fraud	Phar-Mor	1992	Adelphia	2002
Capitalizing expenses, among other issues	Waste Management	1997	WorldCom	2002
Abuse of accounting standards	Savings and loan crisis	1982	Stock options backdating	2006

While the more recent examples presented here began pre-SOX, readers may be skeptical about whether SOX will have its intended effect, especially given the 2008 subprime mortgage and financial institution meltdowns. Further concerns were raised when allegations of misconduct were leveled against Bernard Madoff and Stanford Financial for their Ponzi schemes, costing billions of dollars. While

Ponzi schemes are not new, the sheer magnitude is almost unprecedented, especially in a post–Sarbanes-Oxley world. The investing public was further shocked in January 2009 when news of the Satyam fraud hit the press. In the Satyam case, approximately $1 billion in cash, supposedly the easiest asset to audit, was admitted by the CEO to be nonexistent.

A CLOSER LOOK

Efficiency, liquidity, safety, and robustness of financial markets are vital to the nation's economic prosperity and growth, as more than 110 million Americans directly or indirectly invest in the capital markets. Investors participate in capital markets as long as they have confidence in the quality, reliability, and transparency of public financial information disseminated to the markets. High-quality financial information contained in financial statements prepared by public companies and audited by independent auditors greatly influences investor confidence. Auditor accountability and responsibility for searching, detecting, and reporting financial statement fraud are receiving considerable interest and attention in rebuilding investor confidence and public trust. Until recently, corporate America dismissed financial statement fraud as "irrational irregularities." Now virtually any organization may be affected by financial statement fraud. Not a day passes without fraud-related news, especially in regard to financial reporting. This undermines the quality, reliability, and integrity of the entire financial reporting process and, thus, the efficiency and global competitiveness of our capital markets.

Emerging corporate governance reform, corporate and securities laws, corporate guidance, best practices regulations, and accounting standards are intended to identify and minimize potential conflicts of interest, incentives, and opportunities to engage in financial statement fraud. This chapter (1) addresses financial statement fraud, its definition, nature, and significance; (2) discusses the financial reporting process of corporations; and (3) examines the role of corporate governance, particularly gatekeepers, in preventing and detecting financial statement fraud.

DEFINITION OF FINANCIAL STATEMENT FRAUD

A complete understanding of the nature, significance, and consequences of fraudulent financial reporting activities requires a proper definition of financial statement fraud. *Fraud* is defined in *Webster's New World Dictionary* as "the intentional deception to cause a person to give up property or some lawful right." The legal definition of *fraud* can also be found in court cases. One example of such a definition is "A generic term, embracing all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions by suppression of truth and includes all surprise, trick,

cunning, dissembling, and any unfair way by which another is cheated."[4] Fraud is commonly referred to as an intentional act committed to harm or injure others securing an unfair or unlawful gain.[5] This intentional, wrongful act can be differentiated and defined in many ways, depending on the classes of perpetrators. For example, frauds committed by individuals (e.g., embezzlement) are distinguished from frauds perpetrated by corporations (financial statement fraud) in terms of the classes of perpetrators.

Clear definitions of financial statement fraud are difficult to discern from pronouncements and/or authoritative statements, primarily because it has been only during the past decade that the accounting profession has used the word *fraud* in its professional pronouncements. Previously, the terms *intentional mistakes* or *irregularities* were used. The American Institute of Certified Public Accountants (AICPA, 1997), in its Statement of Auditing Standards (SAS) No. 82, refers to financial statement fraud as intentional misstatements or omissions in financial statements. Financial statement fraud is defined by the Association of Certified Fraud Examiners (ACFE) as:

> The intentional, deliberate, misstatement or omission of material facts, or accounting data which is misleading and, when considered with all the information made available, would cause the reader to change or alter his or her judgment or decision.[6]

The broadly accepted definition of financial statement fraud, which is also adopted in this book, is articulated by the National Commission on Fraudulent Reporting (Treadway, 1987, p. 2) as "intentional or reckless conduct, whether act or omission, that results in materially misleading financial statements."[7]

The common theme among these definitions is that fraud, particularly financial statement fraud, is deliberate deception with the intent to cause harm, injury, or damage. The terms *financial statement fraud* and *management fraud* have been used interchangeably, primarily because (1) management is responsible for producing reliable financial reports, and (2) the fair presentation, integrity, and quality of the financial reporting process is the responsibility of management. Exhibit 1.1 classifies fraud into management fraud and employee fraud and provides further classification of these two types of fraud.

Fraud can be classified into several types, with the most common category being asset misappropriations and financial misstatements. The former is often referred to as employee fraud involving embezzlement, theft of cash or inventory, payroll fraud, or skimming revenues; the latter is viewed as financial statement fraud, usually perpetuated by management. The DoJ defines corporate fraud in three broad areas: accounting fraud or financial fraud, self-dealing by corporate insiders, and obstructive conduct.[8] Accounting fraud consists of falsifying financial information by cooking the books or misleading investors. The most popular accounting schemes are parked inventory sales, side deals, swap transactions, capitalizing expenses, channel stuffing, accelerated revenue, and deferred expenses. Self-dealing by corporate insiders is mostly related to misappropriation of corporate assets by senior

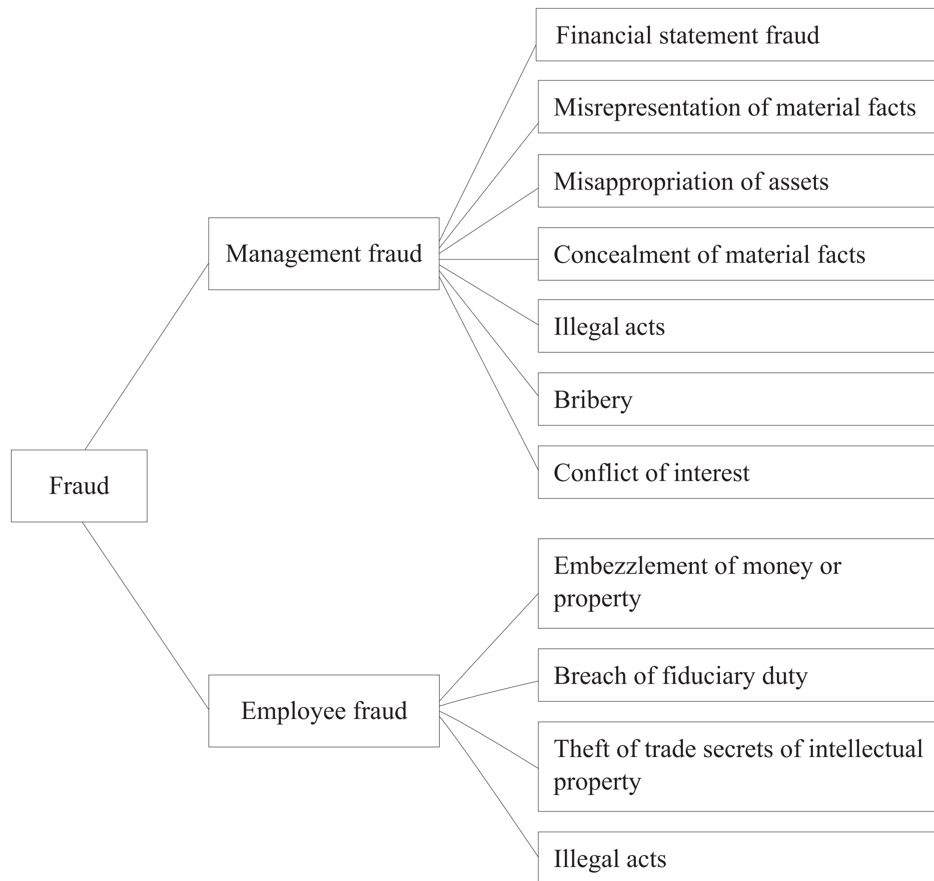


Exhibit 1.1 Types of Fraud

executives, such as loans granted to senior management that are never intended to be repaid, failure to disclose forgiven loans, reimbursed personnel expenses, and extraordinary personnel expenses charged to the company. Other schemes are insider trading, misuse of corporate property for personal gain, kickbacks, and individual tax violations related to self-dealing (e.g., convicted executives of WorldCom and Tyco). Obstructive conduct pertains to criminal penalties associated with falsifying testimony in Securities and Exchange Commission (SEC) depositions, influencing or threatening other witnesses, or lying to criminal investigators (e.g., Martha Stewart's conviction). Other examples of obstructive conduct are erasing computer files, shredding documents, creating or altering documents to support illegal conduct, or intentionally refusing to provide all documents or files required in subpoena.[9]

There are differences in the nature, courses, and determinants of financial statement fraud in the United States and other countries. In the United States, financial statement fraud is commonly caused by management manipulation of earnings to deceive dispersed investors, whereas in Europe, financial statement fraud is

committed to benefit controlling shareholders at the expense of minority shareholders. These differences present challenges to the board of directors, audit committees, external auditors, and regulators in three ways:

1. Fraud prevention and detection methods that are effective in the United States in minimizing financial statement fraud may not work well in the other countries.
2. The primary focus in the United States is on earnings manipulations, which happen less frequently in other countries.
3. Laws, regulations, and standards (e.g., SOX) designed to prevent and detect financial statement fraud may not be effective in other countries to protect investors from fraud.

The focus of this book is on all victims of financial statement fraud, particularly investors and creditors. Thus, the definition of *financial statement fraud* adopted in this book is comprehensive, including both inside and outside victims. It is defined as deliberate misstatements or omissions of amounts or disclosures of financial statements to deceive financial statement users, particularly investors and creditors. In this definition, the class of perpetrators is publicly traded companies; the type of victims is investors and creditors; and the means of perpetration are misleading published financial statements. Financial statement fraud may involve these schemes:

- Falsification, alteration, or manipulation of material financial records, supporting documents, or business transactions
- Material intentional omissions or misrepresentations of events, transactions, accounts, or other significant information from which financial statements are prepared
- Deliberate misapplication of accounting principles, policies, and procedures used to measure, recognize, report, and disclose economic events and business transactions
- Intentional omissions of disclosures or presentation of inadequate disclosures regarding accounting principles and policies in addition to related financial amounts

The five basic elements of fraud are identified as:[10]

1. A false representation of a material nature
2. Knowledge that the representation is false or reckless disregard for the truth (Scienter)
3. Reliance on the false representation by the victim
4. Financial damages are incurred (to the benefit of the perpetrator)
5. An act that was intentional

NATURE OF FINANCIAL STATEMENT FRAUD

Financial statement fraud often starts with a small misstatement of earnings on quarterly financial reports that presumes not to be material but eventually grows into full-blown fraud and produces materially misleading annual financial statements. Financial statement fraud is harmful in many ways:

- Undermines the quality and integrity of the financial reporting process
- Jeopardizes the integrity and objectivity of the auditing profession, especially auditors and auditing firms
- Diminishes the confidence of the capital markets, as well as market participants, in the reliability of financial information
- Makes the capital market less efficient
- Affects adversely the nation's economic growth and prosperity
- May result in huge litigation costs
- Destroys the careers of individuals involved in financial statement fraud, such as top executives banned from serving on the board of directors of any public companies or auditors barred from practice of public accounting
- Causes bankruptcy or substantial economic losses by the company engaged in financial statement fraud
- Encourages excessive regulatory intervention
- Causes destructions in the normal operations and performance of alleged companies

The PricewaterhouseCoopers (PwC) 2005 survey[11] found that accidental ways of discovering fraud through calls to hotlines or tips from whistle-blowers accounted for more than a third of fraud cases, whereas internal audits detected fraud about 26 percent of the time. The survey reported that in the post-SOX era, since 2003, more incidents of fraud have been discovered and reported as evidenced by (1) a 71 percent increase in the reported cases of corruption and bribery; (2) a 133 percent increase in the number of reported money-laundering schemes; and (3) a 140 percent increase in the discovered number of financial misrepresentations. These findings can be interpreted to mean that many corporate governance measures (e.g., internal control, executive certifications, audit committee oversight, whistle-blowing) instituted as a result of SOX have contributed to the discovery of fraud incidents.

The 2008 report of the ACFE[12] included data on how fraud is commonly detected, including the role of the audit committee and internal and external auditors in discovering financial statement fraud. It highlights the need for the audit committee to establish and maintain objective and independent whistle-blowing policies and procedures. It also showed that external auditors should conduct surprise or unpredictable audits on their clients. The report indicated

that among the 237 cases of fraud resulting in a loss of $81 million or more, 16 percent were detected by external auditors, whereas 42 percent were discovered through a tip or a complaint. Frauds in small business were often uncovered through tips by internal auditors and most often by accident. These results suggest that antifraud policies and programs can play an important role in preventing and detecting fraud. Investors commonly assess the lower information risk associated with high-quality financial reports. This lower perceived information risk will make capital markets more efficient and safer and induce lower cost of capital and higher securities prices. Thus society, the business community, accounting profession, and regulators have a vested interest in the prevention and detection of financial statement fraud.

Keith Slotter, assistant director of the Federal Bureau of Investigation (FBI) Training Academy, stated in a January 6, 2006, live Webcast regarding fraud in the post-SOX era: ‘‘People always ask me if it's slowing down, getting better. Nothing has really slowed. It's the same volume as we saw in the initial rush in 2002.’’[13] According to the FBI, in the three years post-SOX, there were more than 400 cases of corporate fraud pending, restitution totaling more than $1 billion; 561 indictments, including 320 c-class executives, 379 convictions, and 3 to 6 new cases opening per month.[14] Corporate fraud in this context is defined as financial statement fraud, obstruction conduct, and self-dealing by corporate insiders, which is occurring more frequently at the end of the reporting periods (quarterly annual reports).[15]

In the post-SOX period July 2002, the DoJ has processed about 1,300 corporate fraud convictions, including convictions of more than 200 CEOs and corporate presidents, 120 corporate vice presidents, and 50 CFOs. These convictions provide evidence of the persistence of corporate malfeasance and accounting scandals, as well as empowerment of federal agencies, regulators, and prosecutors to find, indict, and convict corporate wrongdoers. The number of financial restatements has also significantly increased since July 2002, which suggests a lack of quality and reliability in the previously published statements due to errors, irregularities, and fraud.[16]

Financial statement fraud can be classified into two categories: detected (reported) and undetected. It has been argued that only a small portion of financial statement fraud is detected (reported), and most cases continue until they are discovered. Currently, there is no comprehensive listing of all companies that were engaged in financial statement fraud.

In the past decade, we have confronted many financial scandals and fraud, starting with Enron and WorldCom, among others, market timing and late trading in mutual funds, stock options backdating, the 2008 subprime mortgage crisis, and recent Ponzi schemes. We need to step back to seriously consider and identify what went wrong, decide on what measures are needed to prevent further occurrences of these scandals, understand their impacts on reliability of financial reports, efficiency, and competitiveness of capital markets, and establish ways to ensure investor protection and confidence in our market and economy.

Common themes of reported financial scandals and fraud are the following:

- Lack of transparency and disclosures on complex financial products, including subprime loans, structured finance, off-balance sheet transactions, and credit derivatives
- Lack of accountability, as the financial companies were not responsible through market discipline or by regulators
- Lack of governance and oversight by those responsible for overseeing corporate governance, financial reporting, audit activities, and risk management
- Lack of effective engagement of "gatekeepers," including the board of directors, legal counsel, and internal and external auditors
- Lack of effective analysis by credit rating agencies
- Conflicts of interest and conflicting incentives for corporate directors, officers, and auditors to maximize their interests at the investors' expense
- Opportunities to engage in earnings manipulations and focus on short-term performance
- Incentive structure driven by fees and a process linked to short-term performance rather than sustainable performance
- Lax regulatory environment created by regulators' attempt to follow the "principles-based" regulatory process used in other countries

Market discipline cannot and should not be a substitute for sound, cost-effective, and efficient regulations.

The recent high-profile frauds have raised serious concerns about the following:

- The role of corporate governance, including the board of directors and audit committees
- The integrity and ethical values of these companies' top management teams, especially when CEOs and CFOs are indicted for cooking the books and, in many cases, are convicted
- The ineffectiveness of audit functions in detecting these financial statement frauds
- The substantial declines in the market capitalization of the alleged fraud companies and the likelihood of filing for bankruptcy protection
- Considerable lawsuits by injured investors, creditors, and employees
- Greed and incompetency of some corporate executives
- Efficacy and timeliness of regulation

Regulatory reforms seem to follow a financial crisis:

- Securities Act of 1933 and Security Exchange Act of 1934 were enacted and the SEC was formed in the aftermath of the Wall Street crash of 1929.

- Sarbanes-Oxley was passed in July 2002, pursuant to the reported financial scandal at the turn of the twenty-first century.

HIGH-IMPACT FRAUD CASES

Several key financial statement fraud schemes are summarized next and will be discussed in the next three chapters.

FICTITIOUS REVENUE, DOCUMENTATION FORGERY, AND THEFT OF CORPORATE ASSETS

ZZZZ Best (1987)

Barry Minkow, child genius, started ZZZZ Best as a carpet cleaning service provider at the age of 15 in his family's garage. He was a millionaire by the age of 18.[17] Minkow's company, ZZZZ Best, went public in 1986 and eventually reached a market capitalization of over $200 million. Yet the business scarcely existed and Minkow never ran a profitable operation.[18] To accomplish his goals, Minkow created the perception that he had transformed his company from carpet cleaning to a building restoration business. Minkow set up Appraisal Services, a fake company that verified ZZZZ Best's business dealings. Meanwhile, a ZZZZ Best vice president forged all the documents and contracts necessary to support the jobs. To convince the company's auditor's when they insisted on visiting a restoration job, Minkow went so far as to rent a building and set it up to look like a ZZZZ Best work site.[19]

Enron (2001)

While Enron clearly had more substance that ZZZZ Best, a significant portion of the company's success was built on an elaborate foundation of smoke and mirrors. In 15 years, Enron grew from inception to America's seventh largest corporation, employing more than 21,000 persons in more than 40 countries. But the firm's success turned out to have involved an elaborate scam.[20] While the fall of Enron was due to a failed business model and spin-off ventures in water, international energy brokerage, and broadband communications, Enron's demise began when investors became aware of off-balance sheet partnerships and special-purpose entities that hid billions of dollars of losses. In both Enron and ZZZZ Best, the external auditors maintain that they were deceived by their clients and that important information was withheld.[21]

PERSONAL USE OF ASSETS, FALSE DOCUMENTATION, AND FINANCIAL STATEMENT FRAUD

Phar-Mor (1992)

Mickey (Michael) Monus founded Phar-Mor along with David Shapiro in 1982, based on the philosophy that Phar-Mor buying power gives the customer for more

buying power. It is said that Phar-Mor was one of the few companies that Sam Walton, founder of Wal-Mart, feared as he grew his discount retail mega-giant.[22] Phar-Mor, based in Youngstown, Ohio, filed for Chapter 11 bankruptcy protection on August 17, 1992, after discovering an accounting fraud orchestrated by its top executives. Monus, president and chief operating officer, and Patrick Finn, chief financial officer, covered up approximately $500 million in losses and diverted $10 million in company funds to Monus's World Basketball League. The fraud was concealed through creation of deceptive documentation and manipulated inventory records.

Adelphia (2002)

Adelphia, a cable television company, was founded in 1952 by John Rigas. The company went public in 1986, and by 2000 Adelphia was among the largest cable television and telecommunications providers in the United States. In January 2002, following the collapse of Enron Corporation, the SEC provided guidance regarding disclosures that public companies should consider, including transactions with related parties. Adelphia's disclosures alarmed investors and analysts, leading to a formal investigation by a special committee of Adelphia's board of directors into related party transactions between Adelphia and the Rigases. Adelphia's stock price declined from about $30 per share in January 2002 to $0.30 per share in June 2002, and the stock was delisted from the NASDAQ market. Alleged fraudulent conduct included coborrowing by the Rigases, omission of Adelphia liabilities, and false and misleading financial statements. In addition, members of the family also owned private companies that used Adelphia personnel, inventory, trucks, and equipment to provide services.

CAPITALIZING EXPENSES AND OTHER ISSUES

Waste Management (1997)

Waste Management, Inc. is a waste management, comprehensive waste, and environmental services company in North America. In 1998, an accounting scandal led to a major drop in stock prices and to the replacement of top executives when the new CEO ordered a review of the company's accounting practices. The company had augmented the depreciation time length for their property, plant, and equipment, making their after-tax profits appear higher. The net result was $1.7 billion in inflated earnings.[23] Furthermore, Waste Management refused to record expenses, established inflated environmental reserves (liabilities) in connection with acquisitions, improperly capitalized a variety of expenses, failed to establish sufficient reserves (liabilities) to pay for income taxes and other expenses, avoided depreciation expenses, and failed to record expenses for decreases in the value of landfills as they were filled with waste.[24]

MCI WorldCom (2002)

WorldCom, like Waste Management, was accused of failing to record operating expenses by treating them as capital expenditures and placing them on the balance sheet. WorldCom used two primary techniques: From 1998 to 2000, WorldCom reduced reserve accounts held to cover liabilities of acquired companies, adding $2.8 billion to the revenue line from these reserves. Second, starting in late 2000, operating costs were capitalized as long-term investments, to the tune of $3.85 billion.[25]

ABUSE OF ACCOUNTING STANDARDS

Savings and Loan Crisis (1982)

The savings and loan crisis of the 1980s and 1990s resulted in the failure of 747 savings and loan associations (S&Ls) in the United States. While the major causes of the crisis were believed to be deregulation, imprudent real estate lending, keeping insolvent S&Ls open, brokered deposits, and lower inflation in the U.S. economy, fraud contributed to the problems. Most notably, valueless goodwill was recorded as an asset, and even when goodwill was recorded that appeared initially to have value, subsequent impairments were not recognized. The ultimate cost of the crisis is estimated to have totaled around $160.1 billion, about $124.6 billion of which was directly paid for by the U.S. government.[26]

Stock Options Backdating (2006)

Like the S&L crisis, accounting and securities rules and regulations abuses contributed to the stock options backdating scandal. Issuers of stock options may grant options with any date that they choose. However, when the grant date (the day the options are granted to the recipient) differs from the options stated date, potentially the company would need to recognize compensation expense on the income statement, the company may have disclosure requirements, and the recipient would possibly have personal income tax ramifications. Thus, the issue of backdating is not illegal or problematic, but misleading stockholders, regulators, and the Internal Revenue Service will make backdating illegal.

It is interesting to note how similar the facts and circumstances of earlier high-profile frauds and scandals are to those of more recent events. The similarities show that history does, in fact, repeat itself.

COST OF FINANCIAL STATEMENT FRAUD

The costs to the companies where financial statement fraud is committed can be staggering. The collapse of Enron has caused about $70 billion to be lost in market

capitalization, which is devastating for significant numbers of investors, employees, and pensioners. The WorldCom collapse, caused by alleged financial statement fraud, is the biggest bankruptcy in U.S. history. Loss of market capitalization resulting from the alleged financial statement fraud committed by Enron, WorldCom, Qwest, Tyco, and Global Crossing is estimated to be about $460 billion. These and other corporate scandals have raised three important questions:

1. How severe is corporate misconduct in the United States?
2. Can corporate financial statements be trusted?
3. Where were the gatekeepers, including the auditors?

It is a matter of trust that the majority of publicly traded companies in the United States have responsible corporate governance, a reliable financial reporting process, and effective audit functions, and that they conduct their business in an ethical and legal manner, and through continuous improvements enhance their earnings quality and quantity. The pervasiveness of committed financial statement fraud caused by cooking the books and related audit failures have eroded the public confidence in corporate America.

Fraudulent financial reports are devastating to investors, as they can rock the alleged company's share price. A report by Glass Lewis & Co. shows that investors have suffered significant losses caused by fraudulent financial statements in the past decade.[27] The report indicates the lost market capitalization of 30 high-profile financial scandals caused by fraud during 1977 to 2004 is more than $900 billion and resulted in a negative impact on stock returns for the fraud-prone companies of 77 percent.[28] A recent survey[29] reveals that reported incidents of fraud increased 22 percent worldwide in the past two years with the asset losses of, on average, more than $1.7 million. KPMG's Forensic Fraud Barometer (2005) reported that fraud increased nearly three times in 2005 from the previous year and had the highest recorded level since 1995.[30] Financial statement fraud may constitute a small percentage of the total fraud occurrence, but its cost is definitely the largest with the average annual cost of $250 million.[31]

The actual cost of fraud is difficult, if not impossible, to quantitatively measure for four main reasons:

1. Empirical studies show that only a small portion of all frauds, including financial statement fraud, is discovered.
2. Even if the fraud is discovered, not all cases are reported because companies attempt to preserve their images by firing the fraudsters and pretending that the incident never happened.
3. Fraud surveys in reporting the extent and magnitude of fraud are not always accurate, and they are subject to the limitation of any typical survey study in the sense that the respondents often report their perception rather than the reality.

4. Companies typically do not pursue civil or criminal actions; by firing the fraudsters, many companies believe that they have prevented further occurrences of fraud.

Published statistics on the possible cost of financial statement fraud are only educated estimates; it is impossible to determine actual total costs since not all fraud is detected, not all detected fraud is reported, and not all reported fraud is legally pursued. The reported statistics, however, are astonishing. The ACFE in its "2002 Report to the Nation on Occupational Fraud and Abuse" shows that about 6 percent of revenue, or $600 billion, will be lost in 2002 as a result of occupational fraud and abuse.[32] By 2008, that figure had grown to almost $1 trillion and 7 percent of revenue.[33] The report also found that financial statement fraud was the most costly form of occupational fraud, with median losses of $2 million per scheme.

Other fraud costs are legal costs, increased insurance costs, loss of productivity, monthly costs, and adverse impacts on employees' morale, customers' goodwill, suppliers' trust, and negative stock market reactions. An important indirect cost of financial statement fraud is the loss of productivity caused by dismissal of the fraudsters and their replacements. The top management team is typically involved in financial statement fraud, which forces companies to fire experienced top executives and replace them with less-informed executives. Although these indirect costs cannot possibly be estimated, they should be considered when assessing the consequences of financial statement fraud. Farrell and Healy stated, "The overall cost of fraud is over double the amount of missing money and assets."[34]

Financial statement fraud directly damages investors and creditors who are bound to lose all or part of their investments if such fraud results in a bankruptcy, near failure, substantial reduction in the stock prices, or delisting by organized stock exchanges. Financial statement fraud can also have a significant adverse impact on the confidence and trust of investors, other market participants, and the public in the quality and integrity of the financial reporting process. Decreased confidence in the reliability of financial statements, resulting from fraudulent financial activities, affects all statement users and issuers. Users of fraudulent financial statements will lose because their financial decisions (e.g., investment in the case of investors; transactions for suppliers; employment of employees) are made based on unreliable, misleading financial information. Even a small and infrequent financial statement fraud can affect investors and creditors as well as the public's confidence in the quality of the financial reporting process. Public confidence depends on both the reported actual incidence of financial statement fraud and the perception of the extent that financial statements are threatened by fraudulent activities. Thus, even if the actual level of financial statement fraud may be low, investors and creditors may perceive that the problem exists. Corporate governance must take proper action to improve investor confidence in the financial reporting process.

British East India Company (1600–1874)

Fraudulent financial reporting and corrupt business practices go back to the beginning of the public corporation. While the Dutch East India Company was widely believed to be the first public company, the British East India Company, having started two years prior, in 1600, was also ‘‘taken public’’ with approximately 125 shareholders. The company grew throughout the 1600s. After a period of ferocious speculation following the ‘‘Glorious Revolution’’ in 1688, the company’s share price peaked at approximately £100 in 1693. During the next five years, the share price fell as a result of parliamentary inquiries into allegations of corruption. The stock price bottomed in 1698 when a rival company was established, hitting a low of £39. Scandal again returned to the East India Company in the late 1700s when Edmund Burke had Robert Clive, ‘‘the founder of the empire,’’ and Warren Hastings, India’s Governor-General, brought up on impeachment charges laden with corruption issues. While the trials were failed to convict either man, the company was brought under better parliamentary control. Adam Smith, in his 1776 treatise *Inquiry into the Nature and Causes of the Wealth of Nations*, recognized many of the shortcomings of the modern corporation, including shareholders suffering from extraordinary waste that results from fraud and abuse, a problem inseparable from the management of companies. These problems need not be fatal but need to be consciously and continually scrutinized.

Sources: W. Steve Albrecht, Conan C. Albrecht, and Chad O. Albrecht, ‘‘Fraud and Corporate Executives: Agency, Stewardship and Broken Trust,’’ *Journal of Forensic Accounting* 2004; John Keay, *The Honorable East India Company-A History of the English East India Company* (London: HarperCollins, 1992); Nick Robins, ‘‘This Imperious Company: The English East India Company and Its Legacy for Corporate Accountability,’’ *Journal of Corporate Citizenship* (Spring 2007); Nicholas Dirks, ‘‘What the Scandal of Empire Could Teach the Colonizers,’’ *Financial Times*, July 11, 2006.

FRAUD STUDIES AND REGULATORY RESPONSES

Vigilant and effective corporate governance can substantially reduce the instances of both employee and management frauds and considerably prevent and detect occurrences of financial statement fraud. The fraud studies listed in Appendix: Summary of Six Recent Fraud Studies provide these lessons and implications for corporate governance to prevent and detect financial statement fraud:

- Financial statement fraud is typically perpetrated by top management teams, including presidents, CEOs, CFOs, controllers, and other top executives. Thus, vigilant oversight function of the board of directors and its representative audit committee in (1) setting a tone at the top demonstrating commitment to high-quality financial reports; (2) discouraging and punishing fraudulent financial activity; and (3) monitoring managerial decisions and actions as related to the financial reporting process can substantially reduce instances of financial statement fraud.

- Financial pressures, including substantial declines in both the quality and quantity of earnings, high earnings growth expectations, and an inability to meet analysts' earnings estimates, are often cited in these studies as motivations for management engagement in financial statement fraud. The board of directors and audit committee should:
  - Closely monitor the pressures faced by senior executives
  - Be aware of the gamesmanship practices between management analysts and auditors
  - Attempt to control and monitor such practices
- Ineffective boards of directors and audit committees are cited as important contributing factors that increase the likelihood of the occurrence of financial statement fraud. Publicly traded companies should focus considerably on director independence and expertise as well as qualifications. Companies should comply with the new SEC, New York Stock Exchange, and National Association of Securities Dealers rules on audit committees and should establish vigilant and effective audit committees to oversee the quality, integrity, and reliability of financial reports. These audit committees should be independent, financially literate, well trained and experienced, and actively involved in corporate governance and the financial reporting process to be able to influence the prevention and detection of financial statement fraud.
- Lack of adequate and effective internal control structure has been cited as providing opportunities for the commission of financial statement fraud. The internal control structure can play an important role in preventing and detecting financial statement fraud by reducing the opportunities for perpetration of financial statement fraud and by red-flagging the indicators of financial statement fraud.
- Quality financial audits performed by external auditors are an effective way to reduce the likelihood of fraud occurrence and increase the possibility of fraud detection and prevention. The new O'Malley Panel on Audit Effectiveness suggests the use of forensic-type field work audit procedures on every audit to improve the prospects of detecting material financial statement fraud by external auditors.[35]
- Forensic-type audit fieldwork requires auditors to modify their neutral concept of professional skepticism and presume the possibility of dishonesty at various levels of management, including collusion, gamesmanship, earnings management, override of internal controls, and falsification of financial records and documents. Forensic-type audit procedures are further discussed in Chapter 11.
- These fraud studies reveal that multiperiod financial statement fraud typically starts with the misstatement of interim financial statements. This finding suggests that quarterly financial statements should be thoroughly reviewed by external auditors and, whenever possible, continuous auditing should be performed throughout the year.

- Fraud studies underscore the need for involvement of all corporate governance constituencies, including the board of directors, the audit committee, management, internal auditors, external auditors, and governing bodies as part of a broad effort to prevent and detect financial statement fraud and thus improve the quality, integrity, and reliability of financial statements.
- The Enron debacle, caused by the commission of financial statement fraud, is expected to lead to the following:
  - The establishment of new regulations to improve corporate financial disclosures
  - The requirement of a more effective oversight of public accounting firms
  - The creation of a new accounting industry self-regulating organization that will operate under SEC supervision[36]

SOX was intended to restore the investing public's confidence in corporate America, financial reports, and audit functions. In this context, SOX heightened public and media attention to corporate governance, financial reports, and audit functions. SOX could also have psychological rather than substantive effects. Despite the significance of the substantial effects of SOX, it created what investors could consider as "good news" in revitalizing the capital markets. Many provisions of SOX might have symbolic value and, through signaling effects, influence market participants' confidence in the securities market. Examples of these provisions are as follows:

- Senior executive certification requirements disclosing the already mandated certifications under securities laws
- Real-time disclosure of key information concerning material changes in financial condition or operations signaling the potential business and financial risks in addition to a discussion of their probability and magnitude from management's perspective
- Separation of audit and nonaudit services, which can signal the markets about the objectivity and effectiveness of audit functions as well as resulting impacts on credibility of published audited financial statements
- Improved corporate governance by signaling a more vigilant board of directors and audit committees (e.g., approval of audit and nonaudit services, code of ethics, financial expertise, loans to directors)
- Disclosure controls and procedures provision of SOX requiring public report on management's assessment of controls effectiveness in addition to auditors' attestation and report on management's control assertions
- Whistle-blowing protections for employees who lawfully provide information that they reasonably believe constitutes violations of securities laws
- Increased criminal penalties for violations of securities and other applicable laws and regulations

- Creation of the Public Company Accounting Oversight Board (PCAOB) signaling the improved changes needed in the self-regulatory structure in the auditing profession

These provisions of SOX are classified and summarized in the three overriding areas of corporate governance, financial reporting, and audit functions shown in Exhibit 1.2. The SEC has issued rules in implementing all provisions of SOX, and these rules are discussed throughout the book.

ANTIFRAUD PROGRAMS

Entities of all sizes are susceptible to both employee fraud (e.g., theft, embezzlement) and management fraud (manipulation of financial reports). Effective antifraud programs of focusing on fraud awareness and education in the workplace environment, whistle-blowing policies, and procedures of encouraging and protecting employees who report suspicious behavior, adequate internal control procedures designed to prevent and detect fraud, and conducting surprise audits can significantly reduce fraud. A 2007 survey conducted by Ernst &Young indicates that the majority of respondents (over 68 percent) do not have any antifraud prevention program, and they did not consider their fraud controls to be effective.[37] These results suggest that companies of all sizes should identify and assess fraud risks and design-related antifraud controls, and incorporate antifraud measures into their business operations.

Antifraud programs should be designed and maintained to deter, prevent, and detect all types and sizes of fraud, from misrepresentation of financial information to misappropriation of assets and employee fraud. An effective antifraud program should address corporate culture, control structure, and fraud procedures.

- *Corporate culture*. Corporate culture should create an environment that sets an appropriate tone at the top promoting ethical behavior and reinforcing antifraud conduct, demanding doing the right thing always. The corporate culture provides incentives for everyone in the company, from directors to officers and employees to act competently and ethically.
- *Control structure*. An effective control structure should eliminate opportunities for individuals to engage in fraudulent activities. Section 404 of SOX, SEC rules, and PCAOB auditing standard No. 5 underscore the importance of internal controls in preventing and detecting fraud.
- *Antifraud procedures*. Adequate antifraud procedures should be developed and performed to ensure prevention and detection of potential fraud.

A survey of ethics and workplace conducted by Deloitte & Touche in 2007 finds a strong link between ethics and work-life balance, as 91 percent of respondents felt

Exhibit 1.2 Summary of Provisions of SOX

Corporate Governance	Financial Reporting	Audit Functions	Others
1. Enhanced audit committee responsibility for hiring, firing, compensating, and overseeing auditors and preapproval of nonaudit services 2. Disclosure, in the periodic reports, whether the audit committee has at least one member who is a ‘‘financial expert’’ and, if not, why not 3. CEO and CFO certification of the accuracy and completeness of quarterly and annual reports 4. Management assessment and reporting of the effectiveness of disclosure controls and procedures 5. Ban on personal loans by companies to their directors or executives other than certain regular consumer loans 6. Establishment of procedures by each audit committee for receiving, retaining, and handling complaints received by the company concerning accounting, internal controls, or auditing matters	1. CEO/CFO certification of financial reports 2. Internal control report by management 3. Attestation and report by auditors on management's assessment of internal controls 4. Disclosures of off-balance sheet arrangements 5. Disclosures of contractual obligations 6. Disclosures of reconciliation of non-GAAP financial measures pertaining to pro forma financial information 7. Disclosures of material correcting adjustments by auditors 8. Disclosures of transaction involving management and principal stockholders 9. Accelerated filing of changes in beneficial ownership by insiders 10. Real-time disclosures of information concerning material changes in financial condition or operations (form 8-K disclosures)	1. Establishment and operation of the Public Company Accounting Oversight Board (PCAOB), an independent nongovernmental agency that regulates and oversees the audit of public companies 2. Registration with the PCAOB of public accounting firms that audit public companies 3. PCAOB authority to issue auditing standards, inspect registered accounting firms' operations, and investigate potential violations of securities laws 4. Requirement that auditors be appointed, compensated, and overseen by the audit committee 5. Many nonaudit services are prohibited from being performed contemporaneously with an audit 6. Rotation of the lead (or coordinating) audit partner and the lead review partner every five years 7. Auditors report to the audit committee	1. Professional responsibilities for attorneys appearing and practicing before the SEC 2. Disclosures of corporate code of ethics 3. Collection and administration of funds for victim investors 4. Analyst conflicts of interest (Regulation AC) 5. Whistle-blower protection 6. Debts nondischargeable in bankruptcy 7. Temporary freeze authority for SEC 8. SEC can censure or bar any person who is not qualified, lacks the requisite character or integrity, or with unethical conduct from appearing before the SEC 9. Lengthened statute of limitations for securities fraud 10. Criminalization of corporate misconducts 11. Criminal penalties for defrauding shareholders of public companies 12. Retaliation against informants

7. Review of each quarterly and annual report (forms 10-Q and 10-K) by officers 8. Forfeiture by CEO or CFO of certain bonuses and profits when the company restates its financial statements due to its material noncompliance with any financial reporting requirements 9. Improper influence on conduct of audits 10. Insider trades during pension fund blackout periods 11. Officers and directors bars and penalties for violations of securities laws or misconduct	11. Periodic review of published financial statements by the SEC at least once every three years 12. SEC-enhanced authority to determine what constitutes U.S. GAAP	8. Prohibiting where CEO or CFO previously employed by auditor 9. Auditors attestation to and reporting on management assessment of internal controls 10. Limitations on partner compensation 11. Disclosure of fees paid to the auditor 12. Requirements for preapproval of audit and permitted nonaudit services by the audit committee 13. Retention of audit work papers and documents for five years 14. Increased penalties for destruction of corporate audit records	13. Increased criminal penalties under securities laws and mail and wire fraud 14. Future studies on consolidation of public accounts by firm, audit firm rotation, accounting standards, credit rating agencies, and investment banks

Source: Zabihollah Rezaee, *Corporate Governance and Ethics* (Hoboken, NJ: John Wiley & Sons, 2008), 47.

that workers are more likely to behave ethically at work when they have a work-life balance.[38] Survey results suggest that providing a balance between work and life through a more flexible work schedule provides incentives and opportunities for job satisfaction while fostering an ethical workplace culture. The survey identifies the following five key factors in promoting an ethical workplace:

1. Behavior of management (42 percent)
2. Behavior of direct supervisor (35 percent)
3. Positive reinforcement for ethical behavior (30 percent)
4. Compensation, including salary and bonus (29 percent)
5. Behavior of peers (23 percent)

These results clearly indicate that the majority of respondents (77 percent) believe that the behavior of top management and direct supervisors in setting appropriate tone at the top can significantly foster an ethical workplace environment. Management can create a workplace environment that is conducive to ethical behavior by setting examples and acting as role models for employees to behave ethically. Furthermore, the slight majority of respondents (57 percent) reported that they have observed supervisors setting positive examples of ethical behavior daily or several times per week.

OCCURRENCE, PREVENTION, AND DETECTION

Recently there has been substantial publicity about the extent and magnitude of alleged financial statement fraud that threatens the quality, integrity, and reliability of the financial reporting process and contributes to considerable economic losses by investors and creditors. These financial statement frauds have eroded the public's confidence in the financial reporting process and the audit function. This section describes financial statement fraud occurrence, prevention, and detection.

Exhibit 1.3 illustrates the five stages in which financial statement fraud occurs and can be prevented and detected. At Stage 1, financial statement fraud occurs because management is motivated to mislead financial statement users, particularly investors and creditors. The opportunity for deceptive actions by management exists, and management rationalizes its actions to engage in financial statement fraud. This first stage is thoroughly described and examined in Chapters 2 through 5.

At Stage 2, responsible and effective corporate governance, consisting of a vigilant and active board of directors, an effective audit committee, and an adequate and effective internal audit function, discovers the intended financial statement fraud and prevents its occurrence. If perpetrated financial statement fraud is prevented at this stage, its further damages are eliminated and its adverse effects

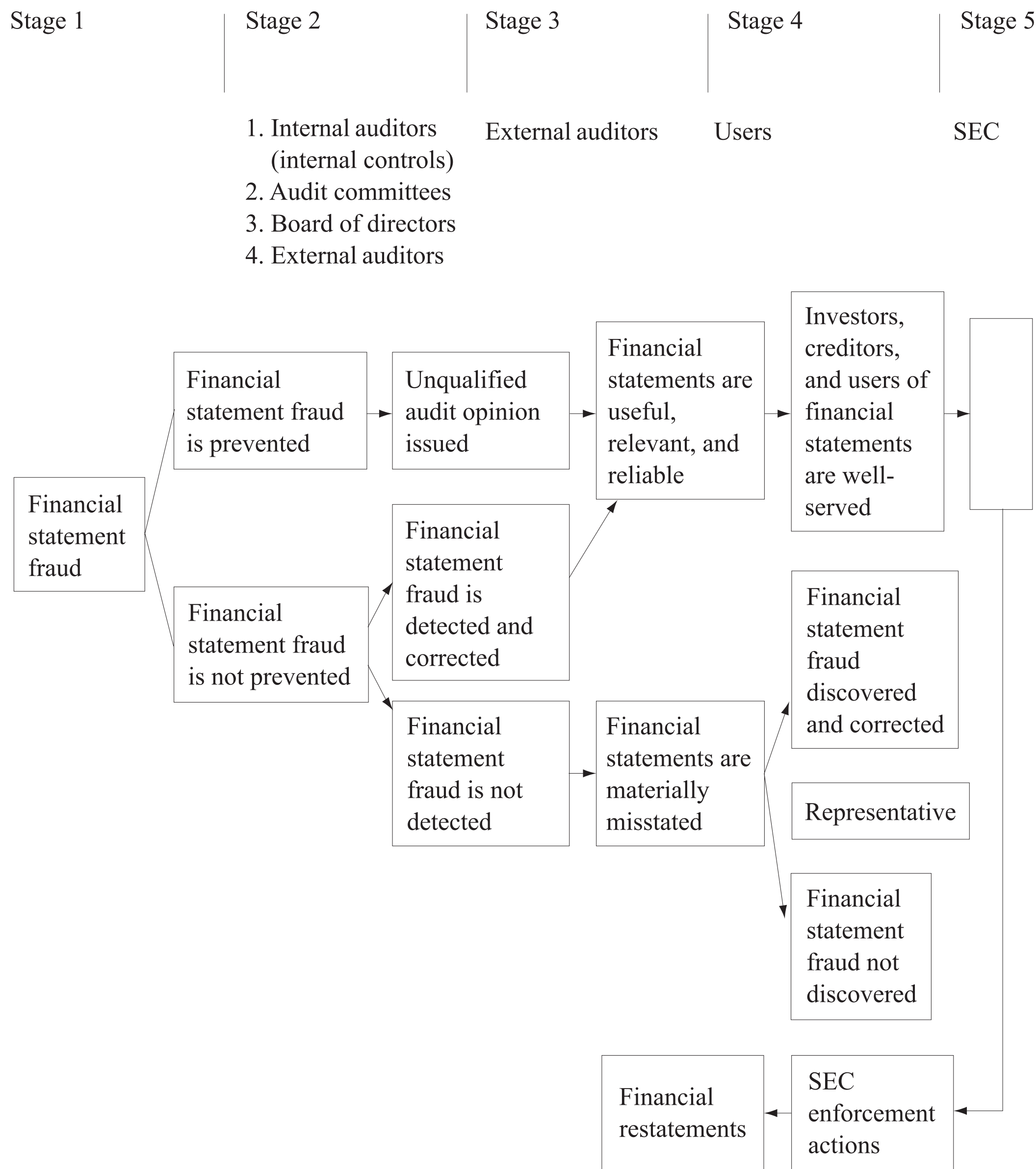


Exhibit 1.3 Financial Statement Fraud Prevention and Detection Process

on quality of financial reports are minimized. However, ineffective and irresponsible corporate governance, along with the gamesmanship attitude of corporate governance, fails to prevent deliberate financial statement fraud perpetrated by management. This stage of the process is described and examined in Chapters 7 through 10.

At Stage 3, financial statements that may or may not contain material misstatements are audited by independent auditors. Independent auditors perform

controls and substantial tests in gathering sufficient and competent evidence to provide reasonable assurance that financial statements are free from material misstatements, including fraudulent activities. When financial statement fraud is detected by independent auditors, the auditors are required to ask management to make corrections. If financial statement fraud is detected by the independent auditors and corrected by the company, then financial statements are fairly presented in conformity with generally accepted accounting principles and portray the company's true financial position, cash flows, and results of operations. Fairly presented financial statements accompanied by an unqualified audit report are considered useful, reliable, and relevant for decision making by investors, creditors, and other users of financial statements. These high-quality financial statements facilitate rational investment decisions and contribute to efficient capital markets. This stage of the process is discussed in Chapter 11.

Financial statement fraud that is not initially prevented and not subsequently detected by independent auditors, accompanied by an unqualified audit report, and disseminated to investors, creditors, and the public, is misleading. At this stage, whether the financial statement fraud is discovered or not, it is considered harmful and detrimental to the integrity and quality of the financial reporting process. This will cause inefficiency in the capital markets, which may result in misallocation of the nation's economic resources.

At the last stage, if financial statement fraud is discovered, either through formal investigations and probes by regulators or informal inquiries by investors, the company will be subject to SEC enforcement actions and will be required to correct and restate misstated financial statements. This final stage is discussed in Chapter 12. The company, its officials, and its auditors then are subject to civil and criminal lawsuit actions or administrative proceedings by the SEC. Any enforcement action by the SEC will have negative effects on the following:

- The reputation, prestige, and status of the alleged company.
- The top management team and other perpetrators of financial statement fraud. The company's officials will be subject to civil penalty, barred from serving on the board of directors or top management team of any publicly traded companies, and subject to criminal prosecutions, including jail time.
- The prestige, reputation, integrity, objectivity, and independence of auditors and auditing firms. Auditing firms may have to pay substantial fines to settle the alleged audit fraud. The partners involved may be subject to fines or be barred permanently or temporarily from auditing public companies.
- The investing public, especially investors and creditors. Investors and creditors may lose their investment substantially if the alleged company goes bankrupt or if stock prices are adversely affected by the alleged financial statement fraud.

- The efficiency of the capital markets through reflection of high financial risk and low-quality financial reports.

LESSONS LEARNED AND APPLICATIONS FOR PRACTICE

Generally, white-collar criminals are intelligent, determined, committed to succeed, highly energetic, creative, good problem solvers, and aggressive. These are the same characteristics of successful entrepreneurs and leaders in business. So what separates professionals from fraudsters, and how do these people avoid the ethical slippery slope that may land them in prison?

The starting point for fraud prevention is "self": "To thine own self be true!" To begin developing an antifraud framework for decision making, a three-pronged approach will assist professionals, managers, board members, auditors, supervisors and staff evaluate decisions:

1. Do you understand what you are being asked to do, the transaction being considered, its economics and related accounting and disclosure?
2. Does any part of the transaction, accounting, or related disclosure purport to hide or conceal important components of the activity from important stakeholders?
3. Does the transaction, accounting, or related disclosure violate basic tenants of ethical decision making?

UNDERSTANDING THE TRANSACTION

It is evident from evaluation of Enron's financial misstatement that the board of directors did not understand the underlying economics of the transactions being proposed by management. While some aspects of the transactions were clearly being hidden by management from the auditors, the audit committee, and the board of directors, none asked for or demanded the necessary information. Consider the Powers Report finding:[39]

> It [the board of directors] cannot be faulted for the various instances in which it was apparently denied important information . . . However, it can and should be faulted for failing to demand more information and for failing to probe and understand the information that did come to light. The Board authorized . . . transactions. It appears that many of its members did not understand those transactions—the economic rationale, the consequences, and the risks.

Thus, the first prescriptive is to get the facts and understand them or ask probing questions until the transaction, proposal, or activity is understood. This advice applies equally to staff, supervisors, managers, executives, and corporate governance

participants. One cannot evaluate, account for, or transparently disclose what one inherently does not understand.

DOES THE ACTIVITY REQUIRE LYING?

Stock options backdating concerned the cherry-picking of the lowest stock price for the period of the options award. Once the selection was made, the Compensation Committee often created minutes or some other document trail to indicate that the option award was made on the date of the lowest closing stock price. The documentation was manufactured to conceal the true date when the options award was actually made. In some cases, the Compensation Committees withheld the release of meeting minutes to ensure that the options award was in fact granted on the date of the lowest stock price.

Concealing one's activities and creating false documentation is a form of lying. At a minimum, lying is considered bad form; in most cases, lying is less than desirable; in some cases, it is illegal. When the activity requires a form of lying, one should stop to question whether the activity is truly appropriate.

BASIC TENANTS OF ETHICAL DECISION MAKING

Violations of ethics, trust, and responsibility are at the heart of fraudulent activities. By their nature, fraud perpetrators are trust violators who have failed to meet their fiduciary responsibility. Trust violators come in two forms: the accidental fraudster and the predator. The predator is one who actively seeks opportunity to steal from others. Upon entry in a new position, the predator searches for the opportunity to achieve his or her goals—typically, financial or economic gain. The primary way to prevent predation is by performing thorough and complete background checks on potential new hires. While such a check may not indicate past transgressions related to fraud, it will likely lead to the realization that the applicant's resume has errors and irregularity or the observation of other anomalies that would normally cause most human resource professionals to question the hire.

By contrast, the accidental fraudster needs not only opportunity but usually acts under some form of distress or duress and has difficulty, at least upon the first fraud act, with the ethical dilemmas associated with fraud. Thus, first-time fraudsters act only if they feel some nonsharable financial or economic problem (pressure or distress) can rationalize the behavior as being for some good cause and have the opportunity to perpetrate the fraud act. These three attributes are known as the fraud triangle: pressure/motive, opportunity, and rationalization. The idea behind the fraud triangle is that it takes all three conditions for the accidental fraudster to perpetrate that first fraud. Internal controls tend to address the opportunity for perpetrators to perceive that they might be able to get away with the proposed scheme. Pressure is an internal characteristic felt by the potential fraud perpetrators, often unobservable to other persons.

Ethics tends to address the rationalization of fraud by considering the conditions under which an action may be considered right or wrong. By explicitly

considering the ethics of a decision, one may be able to persuade potential fraudsters of the error of their ways *before* they initiate their first fraud act. This is important, because once a person becomes a fraudster, he or she seldom self-reforms. Michael Josephson, president of the Josephson Institute of Ethics, suggests several questions with which to evaluate decisions to determine whether you might be on the slippery slopes toward a bad ethical decision:[40]

- If your decision was published on the front page of the local newspaper, would you be proud of your decision or embarrassed, possibly wishing that you would have acted differently?
- What does your gut say? Does the decision you are about to make cause you angst, cause difficulty sleeping, or cause your gut to tighten?
- If your child were with you, observing your action or decision, would you still make the same choice?
- Would this decision or action be something that your mentor, or a person that you admire, approve of?
- What would be the consequences if everyone did what you are considering?
- What if the consequences of your decision were applied to you? How would you feel if you were on the receiving end of the decision or action?

If the answer to any of these questions is less than desirable, you might be on the ethical slippery slope to no-man's land.

SCARED STRAIGHT

Notwithstanding the benefits of doing the right thing to oneself, colleagues, employer, and society, Exhibit 1.4 presents the results of some of the financial scandals discussed earlier in the chapter.[41]

Exhibit 1.4 Sentencing by Scandal and Executive

Company	Executive	Jail Term
ZZZZ Best	Barry Minkow, founder and CEO	Sentenced to 25 years at age 22; served a little over 7 years
Enron	Ken Lay, founder and CEO	Convicted of 25 charges in May 2006 at age 64; died before sentencing, while awaiting appeal
	Jeff Skilling, CEO	Sentenced to 24 years in jail at age 53
	Andrew Fastow, CFO	Sentenced to 6 years at age 46

(*continued*)

(*continued*)

Phar-Mor	Mickey (Michael) Monus, founder and COO	Sentenced to 19 years and 7 months at age 48
	Patrick Finn, CFO	Sentenced to 33 months in jail and testified against Monus
Adelphia	John Rigas, founder and CEO	Sentenced to 15 years at age 80
	Timothy Rigas, CFO	Sentenced to 20 years at age 48
Waste Management	Dean Buntrock, CEO	No charges filed
WorldCom	Bernie Ebbers, CEO	Sentenced to 25 years at age 63
	Scott Sullivan, CFO	Sentenced to 5 years at age 43

Other than Waste Management, Inc., where Dean Buntrock avoided criminal charges, founders and chief executives at each of the other companies will spend or are spending time behind bars. In addition, most had financial fines and community service attributes as part of their sentences.

THE MOST IMPORTANT IMPACT?

Walt Pavlo, perpetrator of a $6 million embezzlement at MCI in the late 1990s, and coauthor Neil Weinberg, may have phrased it best:

> His [Pavlo's] crime seemed victimless. A drop in the bucket for a soulless corporation. It suddenly hit him that the real victims might end up being his wife and sons. . . . The worst day of Pavlo's life came on March 14, 2001, when he kissed his wife Rhoda, Bubby (son age 11) and Howie (son age 9) and headed out the door for the ride to prison.[42]

Wilkie (a coconspirator) told Pavlo that if people knew ahead of time what their crimes could do to their families, they would never commit them.

As part of the Enron scandal, Lea Fastow, wife of Andrew Fastow, CFO, was sentenced to serve one year in an 8-by-10-foot cell in an 11-story jail for signing tax forms she knew included ill-gotten income from her husband's schemes. Lea left behind two young sons at home.

The last thought:

> *In the end, it's only your reputation . . . so manage it wisely.*

NOTES

1. Mark Philip, "Message from the Chairman," 2008 Report to the President: Corporate Fraud Task Force; available at www.usdoj.gov/dag/cftf/corporate-fraud2008.pdf.
2. KPMG Forensic Integrity Survey 2008–2009; available at www.us.kpmg.com/RutUS_prod/Documents/8/IntegritySuvey08_09.pdf.

3. Most of these examples will be examined in more detail in later chapters.
4. *Johnson v. McDonald*, 170 Okl. 117; 39 P.2d 150.
5. W. S. Albrecht, G. A. Wernez, and T. L. Williams, *Fraud: Bringing Light to the Dark Side of Business* (Burr Ridge, IL: Irwin Publishing Co., 1995).
6. Association of Certified Fraud Examiners, *Cooking the Books: What Every Accountant Should Know about Fraud*, No. 92-5401, Self-Study Workbook (Austin, TX: Author, 1995), 12.
7. National Commission on Fraudulent Financial Reporting, ‘‘Report,’’ New York, October 1987.
8. AICPA/FBI Web cast, by AICPA Corporate Financial Insider Staff, ‘‘Small Company Financial Fraud,’’ January 5, 2006.
9. Ibid.
10. The first four elements are presented in Chapter 1 of Thomas W. Golden, Steven L. Skalak, and Mona M. Clayton, *A Guide to Forensic Accounting Investigation* (Hoboken, NJ: John Wiley & Sons), 2006.
11. PricewaterhouseCoopers, ‘‘Global Economic Crisis Survey 2005’’; available at www.pwc.com/ro/eng/ins-sol/survey-rep/PwC_2005_global_crimesurvey.pdf.
12. Association of Certified Fraud Examiners, *2008 Report to the Nation on Occupational Fraud and Abuse*; available at www.acfe.com/documents/2008-rttn.pdf.
13. AICPA/FBI live Web cast.
14. Ibid.
15. Ibid.
16. Corporate Fraud Task Force, ‘‘Report to the President Office of the Deputy Attorney General,’’ Washington D.C., April 2, 2008; available at www.usdoj.gov/dag/cftf/corporate-fraud2008.pdf.
17. Philip Elmer-DeWitt, ‘‘ZZZZ Best May Be ZZZZ,’’ TIME with CNN, July 20, 1987.
18. Joanne B. Ciulla, ‘‘Nothing but ZZZZ Best,’’ *New York Times*, August 8, 2008.
19. Ibid.
20. ‘‘Enron Scandal at-a-Glance,’’ *BBC News World Edition*, August 22, 2002.
21. Peter C. Fusaro and Ross M. Miller, *What Went Wrong at Enron: Everyone’s Guide to the Largest Bankruptcy in U.S. History* (Hoboken, NJ: John Wiley & Sons, 2002).
22. *Frontline, How to Steal $500 Million*, PBS Video, 1992.
23. Reed Kathrein, ‘‘Waste Management Pays for Executives,’’ ‘‘Reed Kathrein’s News on Corporate Fraud,’’ August 30, 2005, available at www.webcpa.com.
24. Steve Albrecht, ‘‘Fraud at Waste Management,’’ AICPA PowerPoint Presentation dated 2003 and 2005; available at the AICPA Web site.
25. Steve Albrecht, ‘‘The Worldcom Fraud,’’ AICPA PowerPoint Presentation dated 2003 and 2005, available at the AICPA Web site.
26. ‘‘Financial Audit, Resolution Trust Corporation’s 1995 and 1994 Financial Statements, GAO Report to Congress, July 1996’’; available at www.gao.gov/archive/1996/ai96123.pdf.

27. Glass Lewis & Co., ‘‘Shareholder Losses from 30 Major Accounting Scandals (1997–2004) Fact Sheet,’’ 2005; available at www.glasslewis.com.
28. Ibid.
29. PricewaterhouseCoopers (PwC), ‘‘Global Economic Crime Survey,’’ 2005; available at www.pwc.com/nz/eng/ins-sol/publications/PwC_2005_global_crimesurvey.pdf.
30. KPMG, ‘‘Massive Surge in Fraud in 2005.’’ Forensic & Litigation Services (January 30, 2005); available at www.kpmg.co.uk/news/detail.cfm?pr=2425.
31. KPMG, ‘‘Fraud Risk Considerations.’’ Audit Committee Institute, 2004; available at www.kpmg.com/aci.
32. ACFE, *2002 Report to the Nation on Occupational Fraud and Abuse*; available at www.acfe.com/documents/2002RttN.pdf.
33. ACFE, ‘‘2008 Report to the Nation.’’
34. R. B. Farrel and P. Healy, ‘‘White Collar Crime: A Profile of the Perpetrator and an Evaluation of the Responsibilities for Its Prevention and Detection,’’ *Journal of Forensic Accounting*, Vol 1, No. 1 (January–June 2000): 17–34.
35. S. F. O’Malley, *The Panel on Audit Effectiveness: Report and Recommendations* (Stamford, CT: Public Oversight Board, August 2000).
36. M. Schroeder, ‘‘Enron Debacle Spurs Calls for Controls,’’ *Wall Street Journal*, December 14, 2001, A4.
37. Ernst & Young, ‘‘From Compliance to Competitive Edge: New Thinking on Internal Control,’’ April 2007; available at www.ey.com.
38. Deloitte & Touche USA, ‘‘Ethics & Workplace,’’ 2007; available at www.deloitte.com/dtt/cda/doc/content/us_ethics_workplace2007a.pdf.
39. William C. Powers, Raymond S. Troubh, and Herbert S. Winoker, Jr., ‘‘Report of Investigation by the Special Investigative Committee of the Board of Directors of Enron Corp. February 1, 2002’’; available at fl1.findlaw.com/news.findlaw.com/hdocs/docs/enron/sicreport/sicreport020102.pdf.
40. Adapted from Arthur L. Berkowitz, *Enron: A Professional’s Guide to the Events, Ethical Issues, and Proposed Reforms* (Chicago, IL, CCH, Inc., 2002).
41. This is not intended to be a comprehensive list of those prosecuted, found guilty, and sentenced.
42. Walter Pavlo Jr. and Neil Weinberg, *Stolen without a Gun: Confessions from Inside History’s Biggest Accounting Fraud* (Florida, Etika Books, 2007), 224 and 262.

Chapter 2

Financial Reporting Structure

INTRODUCTION

The efficiency, liquidity, and safety of the financial markets, both debt and capital, have been threatened by the world economic crisis. This instability has significantly increased the uncertainty and volatility in the markets, which in turn has adversely affected investor confidence. Financial failures such as Enron, Madoff, Satyam, and Stanford Financial started new chapters of fraud and financial scandals, devastating investors' faith in financial reports and in the capital markets. Fraudulent financial reports and financial scandals contribute to uncertainty and market volatility as well as prevent investors from receiving meaningful financial information to make savvy investment decisions.

Consider Enron: the fall of America's "Most Innovative Company." Enron committed financial reporting fraud, but first it was a business failure. Its initial and stunning success was in natural gas marketing. However, in order to fuel revenue and profits growth, Enron attempted to duplicate its success in natural gas by entering new markets. The company ended up trading over 1,800 products in more than a dozen markets in 13 currencies, products including broadband, water, and international energy. Many of those operations, such as EnronOnline (broadband marketing), were unmitigated disasters.[1] When the business model did not work, Enron turned to accounting shenanigans. By the end of 2001, Enron was effectively out of business. Meaningful, reliable, and relevant financial reports are critical trust facilitators that help fuel the world's financial markets; their importance cannot be overstated.

FINANCIAL REPORTING SYSTEM

The financial reporting system is a complex process that is influenced by a variety of factors, including technological, political, cultural, economic, and business environments. The National Commission on Fraudulent Financial Reporting, better known as the Treadway Commission, has broken down the financial reporting system into three fundamental elements:

1. Companies and their directors and officers
2. Independent public accountants
3. Oversight bodies[2]

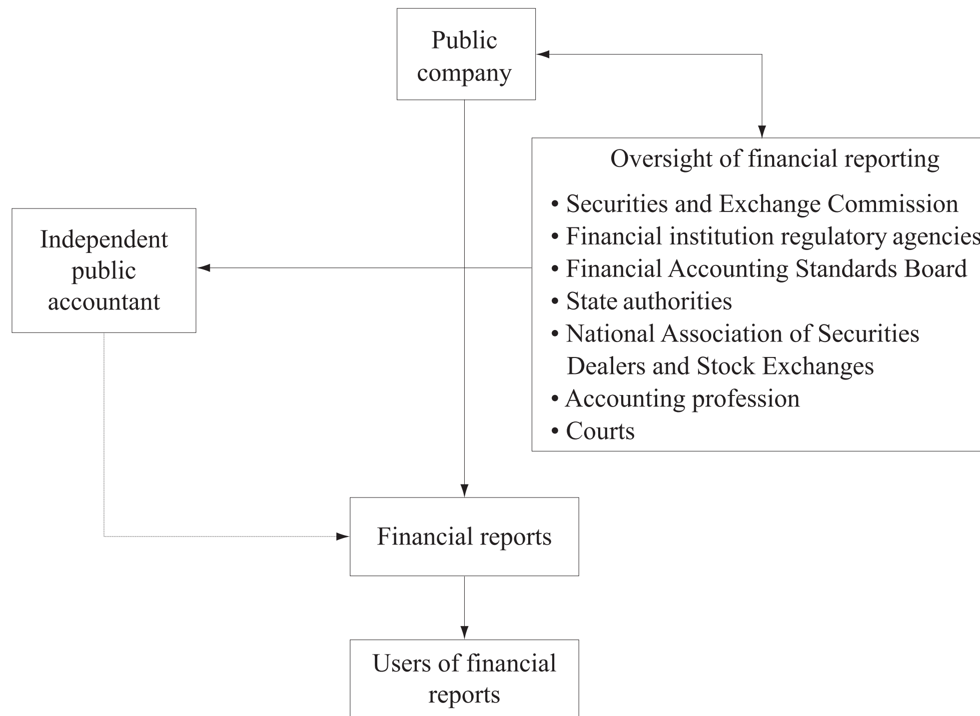


Exhibit 2.1 Financial Reporting System
Source: Adapted from the Treadway Commission Report (www.coso.org).

Exhibit 2.1 describes the relationships of the three fundamental elements of the financial reporting system and their interactions with the users of such a system. A company and its directors as well as senior management play important roles in the financial reporting system and process. They are primarily responsible for fair and true presentation of financial reports conforming to established criteria known as reporting standards. The integrity and quality of financial reports reflect management commitment and intent in preparing and disseminating reliable, relevant, and useful information about the company's financial position, results of operations, and cash flows. The board of directors and its representative audit committee oversee the financial reporting process even though management actually prepares and certifies the financial statements. Senior executives of large public companies in compliance with Section 404 of the Sarbanes-Oxley (SOX) Act also prepare and certify the company's internal control over financial reporting (ICFR) in addition to certification of financial statements.

Independent public accountants, by virtue of being independent and knowledgeable, are engaged to render an opinion regarding the fair presentation of financial reports on the company's financial position and the results of operations in conformity with generally accepted accounting principles (GAAP). Independent public accountants lend more credibility and objectivity to published financial statements by reducing the information risk. Information risk is the probability that published

financial statements may be inaccurate, biased, false, incomplete, and/or misleading. Independent auditor responsibilities in opining on both financial statements and internal control over financial reporting of public companies in the post-SOX are defined and governed by auditing standards issued by the Public Company Accounting Oversight Board (PCAOB).

Several oversight bodies influence a set of financial reporting standards for public companies and also monitor and enforce compliance with those standards. These oversight bodies consist of the Securities and Exchange Commission (SEC), Financial Accounting Standards Board (FASB), state authorities, courts, and accounting profession. The SEC, in fulfilling its responsibility for administering the federal securities laws, establishes disclosure requirements for public companies. Traditionally, the SEC has maintained its oversight responsibility over the financial reporting of publicly traded companies while, in most cases, it delegates its authority for establishing accounting standards to private sectors such as the FASB. In the post-SOX era, the PCAOB governs and regulates public company auditing firms.

IMPORTANCE OF FINANCIAL INFORMATION

Reliability, transparency, and quality of financial information are the lifeblood of the capital markets. The efficiency of the markets depends on the reliability of that information, which enables the markets to act as signaling mechanisms for proper capital allocation. A greater number of people are now investing through retirement funds or are actively managing their portfolios. Therefore, they are affected by the financial information disseminated to the market. Reliable and transparent financial information contributes to the efficient functioning of the capital markets and the economy. WorldCom and Enron, the two biggest corporate bankruptcies in U.S. history, raise serious concerns about the value-adding activities of public companies' corporate ethics and governance as well as the professional accountability of the board of directors, senior management, internal and external auditors, and other corporate governance participants. The lack of public trust and investor confidence in corporate America and its financial reports has continued to adversely affect the vibrancy of the capital market: "Enron has left us with a legacy of mistrust."[3] This legacy has challenged business leaders to change their culture, behavior, and attitudes to restore public confidence and trust in business.

Enron's Accounting Irregularities

Enron used three primary accounting shenanigans:

1. *Mark-to-model accounting.* In the natural gas market, Enron marketed stable financial contracts to its customer by combining derivatives: options, swaps, and similar financial instruments. The problem at Enron was that many of its contracts were custom-designed and did not have a ready market. Custom contracts without a market are difficult to value so Enron valued these contracts through computer models, a process known as mark-to-model. These values are not market, they are simply sophisticated estimates and an opportunity for

(*continued*)

fraud—Enron could put a positive spin on its earnings. The end result: Enron not only started to believe that mark-to-model earnings were real but also manipulated the models to create fictitious earnings.

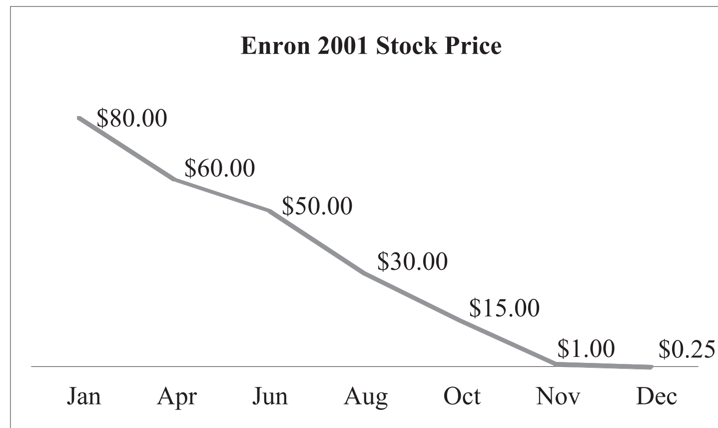
2. *Use of off-balance sheet special-purpose and other related party entities.* When an entity, such as the New York Stock Exchange (NYSE), acts as a market marker, it has no ownership positions in the assets and liabilities being traded; instead, the market maker assists willing buyers and willing sellers to meet in an effective, efficient, and low-cost manner. The trouble with Enron was that in many of its markets, the company took an ownership position in the assets being traded. The company's ownership of its inventory of energy and other assets also created enormous debt. Enron used about 500 special purpose entities (SPEs) and thousands of questionable partnerships in order to structure transactions to achieve off-balance sheet treatment of assets and liabilities. Because the SPEs and partnerships were kept out of their financial statements, Enron's risk related to the credit obligations, massive debt, and various guarantees remained hidden by a veil of deception. When its guarantees came to light during 2001, the market's trust in Enron's ability to deliver as a market maker evaporated. Even more interesting was that Enron executives had significant financial stakes in some of these SPEs and personally reaped huge income from that ownership. For example, Andrew Fastow, chief financial officer, is reported to have made more than $30 million and Michael Kopper, a Fastow assistant, is reported to have made at least $12 million on their related party investments in Enron off-balance sheet entities.[4]
3. *Sale of company stock treated as accounts receivable.* In 2000, Enron created four SPEs. As part of the initial capitalization, Enron issued its own common stock in exchange for notes receivable. At the time, Enron increased notes receivable (an asset) as well as shareholders' equity to reflect these transactions. However, GAAP generally requires that notes receivable arising from transactions involving a company's capital stock be presented as deductions from stockholders' equity, not as assets. Enron has indicated that it overstated both total assets and shareholders' equity by approximately $1 billion between June 2000 and March 2001.

Even with these accounting mistreatments, Enron was demonstrating signs of impending financial meltdown. In the first and second quarter of 2001, Enron reported negative cash flows from operations in contrast to positive operating earnings—not a sign of financial health. (see Exhibit 2.2)

The management of large public companies is being held more accountable for the effectiveness of internal controls and integrity of financial statements through regulations such as SOX (e.g., executive certification). Global investors are provided with integrated financial and internal control reports (IFICRs) prepared by management and audited by independent auditors. These integrated reports should be useful to investors because an effective ICFR is vital in preventing and detecting financial misstatements, including fraud. Exhibit 2.3 presents the framework for an IFICR. An IFICR includes five elements:

1. Management report and certification of financial statements
2. Management report and certification of an ICFR
3. The independent auditor's opinion on the fair and true presentation of financial statements

Exhibit 2.2 Summary of Enron 2001 Activities and Stock Price



January	During the first week of January, the revelry and celebration was an Enron theatrical event where champagne and liquor flowed: Kenneth L. Lay strode onto a ballroom stage at the Hyatt Regency Hill Country Resort in San Antonio, TX, between two giant screens that displayed his projected image,[i] Lay said the company would take on a new mission: Enron would become "the world's greatest company." Behind the theatrical pageantry, Enron was quietly falling apart.[ii]
February	Enron executives get bonuses worth millions. *Fortune* magazine names Enron the most innovative company in America for the sixth straight year.
March	In a March 8 memorandum, Jordan Mintz, Enron's lawyer, expresses concerns about some of Enron's deals.[iii] Later that month, to avoid issues associated with the falling stock price, Enron repurchases one special-purpose entity's interest in another for $35 million, netting Michael Kopper, one of CFO Fastow's underlings, $10 million in profits.
April	Enron reports $542 million in operating income but more than $400 million of operating cash flow losses.
May–June	While Enron is accused of being instrumental in California's energy crisis, Chief Executive Officer Jeffrey Skilling makes a joke in Las Vegas: "What's the difference between the *Titanic* and California? . . . The *Titanic* went down with the lights on!"
July–August	Enron announces second-quarter operating profit of $676 million but operating cash flow losses of $873 million. Jeff Skilling resigns from his "dream job" as Enron's CEO. Kenneth Lay, Chairman of the Board, replaces Skilling. On August 15, Sharon Watkins anonymously writes her now-famous memo to Ken Lay. The memo is known for its first sentence: "Has Enron Become a Risky Place to Work?"
September–October	Andersen, Enron's auditor, discovers that incorrect entries increased Enron's stockholders' equity by $172 million in the first-quarter of 2000 and by $828 million in the first quarter of 2001, requiring that the $1 billion error be corrected.

(*continued*)

Exhibit 2.2 (*continued*)

	The SEC initiates an investigation.
	Andrew Fastow, CFO, resigns.
	Enron reports third-quarter losses of $618 million.
November	Enron announces that it overstated profits by $586 million over five years.
	Enron attempts to negotiate a bailout with Dynergy that fails.
	Enron's credit rating is lowered and it collapses under a mountain of debt while hemorrhaging cash.
December	Enron files for bankruptcy and lays off 4,000 employees.

[i] K. Eichenwald and D.B. Henriques, "Enron's Many Strands: The Company Unravels; Enron Buffed Image to a Shine Even as It Rotted from Within," New York Times, February 10, 2002.

[ii] David M. Boje, "Theatres of Capitalism," December 12, 2001; available at http://cbae.nmsu.edu/~dboje/theatrics/theatrics.htm.

[iii] Richard A. Oppel, Jr., "Enron's Many Strands: Early Warning; Lawyer at Enron Warned Officials of Dubious Deals," New York Times, February 7, 2002.

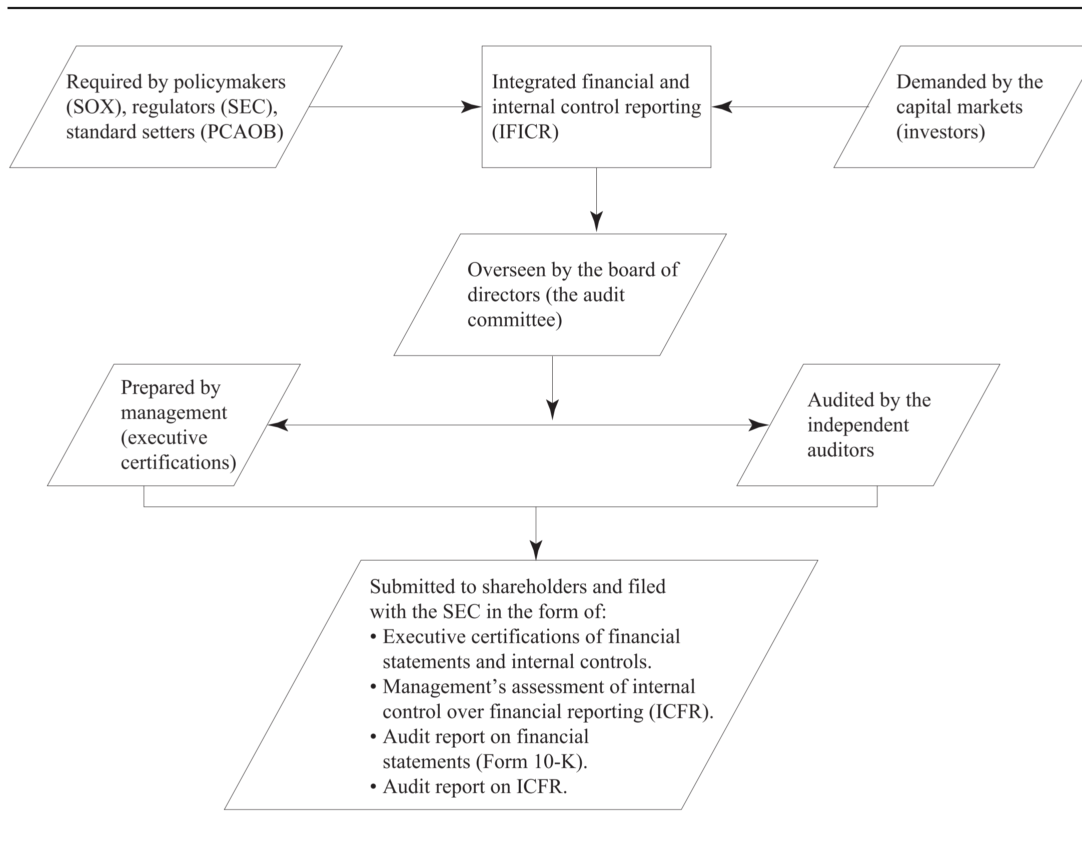


Exhibit 2.3 Framework of the Integrated Financial and Internal Control Reporting (IFICR)

4. Independent auditor's opinion on the effectiveness of the ICFR
5. The audit committee's review of audited financial statements and both management and auditor reports on the ICFR

The effectiveness of the IFICR depends on the following:

- A vigilant oversight function by the board of directors, particularly the audit committee
- A responsible and accountable managerial function by senior executives
- A credible external audit function by the independent auditor
- An objective internal audit function by internal auditors

FINANCIAL REPORTING PROCESS

Information from public companies flows into the marketplace from three fundamental sources:[5]

1. Regulated disclosures
2. Voluntary disclosures
3. Research analyst reports

Regulated disclosures include filings with the SEC of annual audited financial statements on the 10-K Form, quarterly reviewed financial reports on Form 10-Q, extraordinary transactions on a current basis on the 8-K Form (e.g., auditor changes, resignation or death of a director or an officer, bankruptcy), and internal control reports for large public companies (Sections 302 and 404).

Public companies often voluntarily release earnings guidance regarding projected performance as well as other financial and nonfinancial information in addition to their mandated disclosures. Earnings announcements, even though not required, provide valuable information to market participants and motivate companies to meet their earnings expectations. Voluntarily released earnings guidance is expected to result in higher valuations, lower volatility, and improved liquidity.

Financial analysts who follow and project companies' future earnings and evaluate their short-term quarterly performance are an important source of information and are essential to transparent and efficient capital markets. Analysts forecast for both long-term and short-term earnings quality and quantity. The mere focus on short-term analysts' forecasts and quarterly earnings guidance when such earnings numbers can be easily manipulated through either acceleration of revenue recognition or deferral of investments (e.g., technology, research and development) can cause erosion in investor confidence regarding the quality of earnings releases

The current system of financial disclosures—which consists of mandated disclosures of quarterly, annual, and other filings with the SEC; voluntary disclosures

of earnings guidance above and beyond the required disclosures by the SEC; and analyst reports—has served the capital markets, investors, public companies, and regulators well.

ANNUAL FINANCIAL REPORTING REQUIREMENTS

A company's annual report is typically the primary means of communication with current as well as potential investors and creditors. Thus, management attempts to use this vehicle to portray the company in a favorable manner by adding "gloss" to the annual report while complying with the reporting requirements set forth by the SEC.

Rule 14a-3 of the Securities Exchange Act of 1934 requires that annual reports provided to shareholders in connection with the annual meetings of shareholders include the following:

- Audited financial statements consisting of balance sheets as of the two most recent fiscal years
- Statements of income
- Cash flows for each of the three most recent years

In addition, Rule 14a-3 requires that the following information, as stated in Regulation S-K, be included in the annual report to shareholders:

- Selected quarterly financial data
- Summary of selected financial data for last five years
- Segment information
- Management's discussion, analysis of financial condition, and results of operations
- Quantitative and qualitative disclosures about market risk
- Market price of company's common stock for each quarterly period within the two most recent fiscal years
- Description of business activities
- Disagreements with accountants on accounting and financial disclosure

SOX Section 301 and the related SEC implementation rules require an audit committee report to be published annually in the proxy statements for annual meetings of shareholders. This report should state whether the audit committee has completed these activities:[6]

- Reviewed and discussed the audited financial statements with management
- Received from the auditor a letter disclosing matters that, in the auditor's judgment, may reasonably be thought to bear on the auditor's independence from the company and discussed with external auditors their independence

- Recommended to the board of directors that the company's audited financial statements be included in the annual report on Form 10-K or Form 10-KSB

HIGH-QUALITY FINANCIAL REPORTS

The SEC, since its inception more than 75 years ago, has continued to protect investors through the fair and orderly operation of the capital markets. High-quality and transparent financial reports prepared based on full and fair disclosures promote efficient capital markets. Certain qualitative aspects of financial information are important in producing high-quality and transparent audited financial statements that are prepared in conformity with GAAP.

The Statement of Financial Accounting Concept (SFAC) No. 1, "Objectives of Financial Reporting by Business Enterprises," promulgated by the FASB in 1978, states that:

> Financial reporting should provide information that is useful to present and potential investors and creditors and other users in making rational investment, credit, and similar decisions. The information should be comprehensible to those who have a reasonable understanding of business and economic activities and are willing to study the information with reasonable diligence.[7]

The financial reporting model that has been established through the continued efforts of both the public and private sectors is designed to provide users, particularly investors and creditors with useful, reliable, relevant, comparable, consistent, and transparent information that is necessary to make informed and educated financial decisions.

Management, specifically the chief financial officer, is primarily responsible for fair presentation of financial statements in conformity with GAAP that portray the company's performance, cash flows, and financial position to investors, creditors, and other users of financial statements. SFAC No. 2 describes nine qualities and characteristics that make financial information useful for decision making by all users of financial statements.[8] The additional characteristic of transparency has been added to this list of nine characteristics:

1. *Relevance*. The financial information is viewed to be relevant if it makes a difference to the decisions made by decision makers (e.g., investors, creditors) and helps users to:
   - Assess past performance
   - Predict future performance
   - Confirm or correct expectations
   - Provide feedback on earlier expectations

   Relevance, which encompasses the concepts of predictive value, feedback value, and timeliness, indicates that information is relevant when it is capable of making a difference in a decision.

2. *Timeliness*. Timeliness means providing financial information to decision makers when they need such information and before the information loses its capacity and capability to influence decisions. It has been argued that historical financial statements do not provide timely, relevant information for investors and creditors to make investment decisions. Thus, online, real-time electronic financial reports have been suggested to improve the timeliness of financial information. Extensible business reporting language (XBRL) and Internet-based financial reports, which are discussed in depth in Chapter 12, also enhance the timeliness of business reports.
3. *Reliability*. Financial information is reliable when investors and creditors consider the information to reflect economic conditions or events that it purports to represent. Reliability, which encompasses the notions of verifiability, neutrality, and representational faithfulness, is a measure of the integrity and objectivity of financial reports. Reliability provides assurance for users that the information is accurate and useful.
4. *Verifiability*. Verifiability is the extent to which different individuals using the same measurement material arrive at the same amount or conclusion. For example, cash is considered a verifiable financial item because different individuals can count the reported cash and reach the same conclusion about the ending balance of cash.
5. *Representational faithfulness*. Representational faithfulness means the degree of correspondence between the reported accounting numbers and the resources or events those numbers purport to represent. Representational faithfulness of published audited financial statements means the extent to which they reflect the economic reality, resources, and obligations of the company, as well as the transactions and events that change those resources and obligations.
6. *Neutrality*. High-quality financial information should be neutral in the sense that it is free from bias toward a predetermined result. Neutrality implies that management, in using its discretion to choose among a set of acceptable accounting methods, should select the method that reports the economic reality of the transactions or events.
7. *Comparability and consistency*. High-quality financial statements require the use of standardized and uniform accounting standards and practices for measuring, recognizing, and disclosing similar financial transactions or economic events. The reported financial information of a particular company can be considered useful for decision making if the decision maker (e.g., investor, creditor) can compare it with similar information about other companies and with similar information about the same company for some other time period. Comparability and consistency suggest that comparability of information among companies and consistency in the application of methods over time enhances the information value and value relevance of financial reports.
8. *Materiality*. An amount or a disclosure is considered to be material if it influences or makes a difference to a decision maker. Materiality affects the quality,

integrity, and reliability of financial statements, because management uses its judgment to decide what may be material to users of financial statements. Auditors use materiality judgment in determining the type of audit report to produce when there is a departure from GAAP. Materiality threshold used by management in presenting financial information has been challenged by the SEC in many of the alleged financial statement fraud cases filed against publicly traded companies.

9. *Feasibility or costs and benefits*. High-quality financial information or disclosure must be feasibly practical and cost effective. Management, in deciding about a particular disclosure or implementation of a particular control activity, considers whether the perceived benefits to be derived from the decision exceed the perceived costs associated with it.
10. *Transparency*. High-quality financial information must be transparent in the sense that it provides the complete reporting and disclosure of transactions, which portray the financial conditions and operational results of the company in conformity with GAAP. Transparency enables financial statement users, including investors and creditors, to obtain the right information and ensure that financial information is factual and objective. The more transparent the financial reporting process, the easier it is to obtain and assess the nature of the transactions as well as the quality of the related financial statements.

SIX-LEGGED STOOL OF THE FINANCIAL REPORTING PROCESS

High-quality financial reports, including reliable financial statements free of material misstatements caused by errors and fraud, can be achieved when there is a well-balanced functioning system of corporate governance, as depicted in Exhibit 2.4. This system comprises six participants:

1. Board of directors
2. Audit committee
3. Top management team
4. Internal auditors
5. External auditors
6. Governing bodies, including the SEC, PCAOB, American Institute of Certified Public Accountants (AICPA), NYSE, and National Association of Securities Dealers (NASD)

These participants develop a six-legged stool that supports responsible corporate governance and reliable financial reports. Although the responsibilities of these participants will vary regarding preparation and dissemination of financial statements, a well-defined cooperative working relationship among these participants

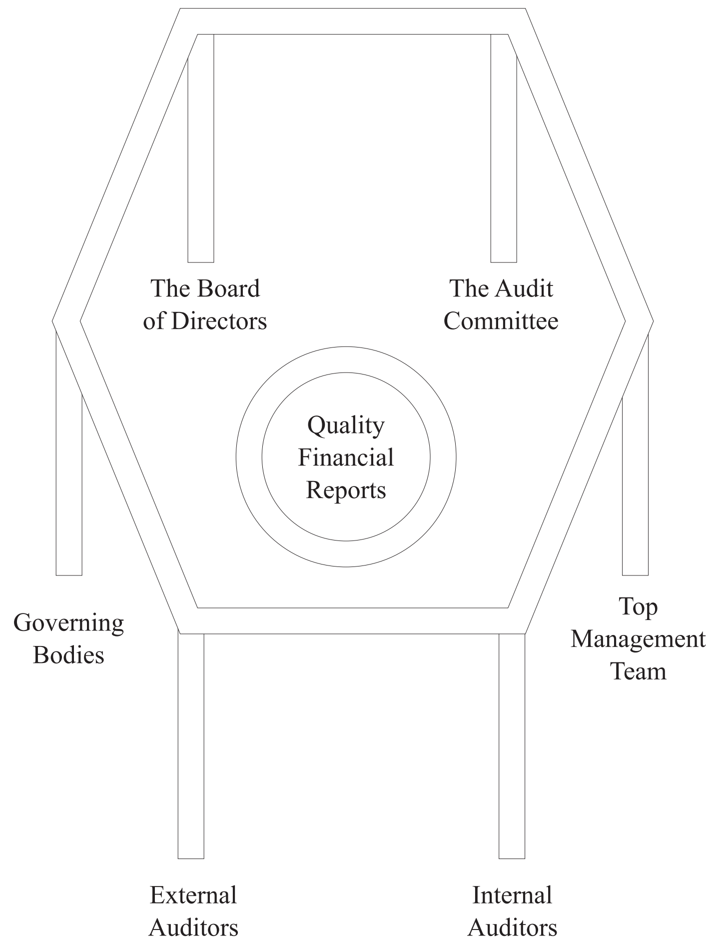


Exhibit 2.4 Six-Legged Stool of the Financial Reporting Process

should reduce the probability of financial statement fraud. The responsibility of these participants in ensuring corporate governance and reliable financial statements is thoroughly examined in Chapters 6 through 12. Fair presentation of financial statements, and the representational faithfulness, verifiability, soundness, and neutrality of the financial information, is the primary responsibility of the top management team. The board of directors and its representative and extension, the audit committee, have the ultimate oversight responsibility of the financial reporting process. The auditors lend more credibility to financial reports while governing bodies establish guidance for financial reporting.

CORPORATE FINANCIAL REPORTS

Companies listed on stock exchanges are required to publish annual and quarterly financial reports, including the three fundamental financial statements:

1. Statement of financial position, which is better known as the balance sheet
2. Income statement
3. Statement of cash flows

Company financial reports typically consist of the following:

- The three fundamental financial statements
- Statement of changes in owners' equity
- Notes to the financial statements
- Auditor's report
- Five-year comparative summary of key financial items
- Management's discussion and analysis of operations
- High and low stock price
- Other financial and nonfinancial information

To achieve the target performance, management may attempt to report favorable financial results on the financial statements prepared in accordance with GAAP and accompanied with a clean standard audit opinion. When ''true'' financial results are favorable and meet investors' expectations conveyed through analysts' forecasts, companies have the incentive to be more legitimate and ethical and are less motivated to engage in fraudulent financial reporting. However, when ''true'' financial results are less favorable or unfavorable, the firm may choose one of these alternatives:

- Issue unfavorable financial results that are in compliance with GAAP
- Violate GAAP to report more favorable financial results
- Engage in fraudulent financial activities to report more favorable financial results

Adoption of any of these alternatives has a cost to the company and its executives and management.

In the emerging digital knowledge–based economy, financial statement users, particularly market participants, need (1) more disclosure of key performance indicators (KPIs) on financial and nonfinancial information, (2) more forward-looking financial information, and (3) more information about intangible assets. It is expected that the U.S. financial reporting process will eventually be based on a single set of high-quality accounting standards as issued by the International Accounting Standards Board (IASB). The efficiency and competitiveness of U.S. capital markets depends on the ability of financial statement preparers to effectively communicate with investors through financial reports. This effective communication can be impaired by complexity and lack of transparent and reliable

financial reports. The past decade has witnessed widening attention on accountability and social responsibilities of corporations caused by a wave of global financial scandals at the turn of the twenty-first century. It has also led to the growing demand for corporate accountability on issues ranging from economics to social responsibilities. The demand for more transparent corporate reporting reflecting economic, social, governance, ethical, and environmental sustainable performance is increasing in the context of sustainability reporting. Corporate reporting is often referred to as sustainability reporting, corporate social responsibility, or multiple bottom-lines (MBL) reporting. Corporate reporting focuses on both financial and nonfinancial key performance indicators (KPIs) to ensure corporations are held accountable and are fulfilling their responsibility in managing their affairs in a fair and transparent fashion.

How Does $50 Billion Disappear?

Bernard Madoff ran an investment fund that serviced pensions, institutional investors, and endowments, in addition to the rich and famous. As it turns out, it was all a Ponzi scheme. In December 2008, according to the SEC, Madoff admitted to stealing $50 billion. In February 2009, it was revealed that Madoff had purchased no securities at all for at least the past 13 years. How does $50 billion just vanish?

The firm was Bernard L. Madoff Investment Securities LLC, and it reported steady monthly returns of approximately 1 percent for nearly two decades. When someone is successful, no one wants to look too closely at his activities. Given that Madoff had the trust of wealthy persons, universities, charities, and other investment fund managers, due diligence was not performed. For decades, Madoff was well known on Wall Street and had an impeccable reputation for success. In addition, he emphasized secrecy and exclusivity. Investors were more afraid of not being invited to invest than they were about the risk of losing money. With this country club mentality, his activities were not very well scrutinized.

Even when allegations were made and opportunities to examine Madoff's LLC arose, those responsible failed to unveil what was really going on. The SEC and lawmakers are trying to understand these failures. While some of the $50 billion may ultimately be found, most likely investors will get little money when all is said and done.

Sources: Jason Zweig, "How Bernie Madoff Made Smart Folks Look Dumb," *Wall Street Journal*, December 13, 2008; Zachary Goldfarb, "SEC Broadens Its Probe of Failures in Madoff Case," *Washington Post*, January 6, 2009.

CORPORATE REPORTING CHALLENGES

Some of the persistent and emerging financial reporting challenges that may threaten the integrity and quality of financial reporting are presented in this section.

PRESSURE TO MANAGE EARNINGS

Publicly traded companies are pressured to report earnings that meet analysts' forecasts and expectations rather than focusing their efforts on continuously improving quality and quantity of earnings, primarily because (1) missing the earnings expectations mark can cost a significant amount of dollars in the market capitalization, and (2) top management compensation, including bonuses, is linked to the reported earnings. The high market capitalization and significant valuations of equity securities during the late 1990s have created pressures on management to achieve earnings estimates or other performance targets typically determined by security analysts. The efficiency and competitiveness of the capital markets, in reflecting publicly available information into stock prices, have encouraged companies to achieve these targets, either by continuously improving their performance and thus creating shareholder value, or by attempting to make the numbers seem more positive and thus engaging in financial statement fraud.

EXCESSIVE AND IMPROPER USE OF FINANCIAL DERIVATIVES

Financial derivatives and complex financial instruments have grown rapidly during the past two decades, primarily because of fundamental changes in global financial markets, advances in computer technology, fluctuations in interest and currency exchange rates, the creativity of financial engineers, and a lack of guidance, regulation, and oversight. Derivatives are sophisticated financial instruments tied to the performance of underlying assets and have been used for a variety of purposes, including risk management, financial schemes, tax planning, earnings, management, and speculation activities. However, the nature of risks associated with derivatives and how corporations use them are not well understood, either by the creators of these instruments or users of financial statements. The financial community and regulators are concerned with complexities, risks, lack of uniform accounting practices for derivatives, and inadequate reporting of their fair values. The excessive and improper use of derivatives has led to the creation of misleading and fraudulent financial statements.

FINANCIAL RESTATEMENTS

About 10 percent of listed U.S. public companies restated their financial statements in 2006. Financial restatements hit a new record in 2006, as 1,356 public companies filed 1,538 restatements, which was up 13 percent compared to 2005. Hranaiova and Byers,[9] in a PCAOB-sponsored study, found overall negative capital market reactions to restatement announcements in both the pre- and post-SOX period, while the extent of reactions (either positive or negative) was reduced in the post-SOX period, along with lower average volatility. They interpreted their findings to mean that investors, in the post-SOX era, consider restatements to convey

timelier and higher-quality information. SOX, by emphasizing internal control, has made both executives and auditors more conservative and more likely to find errors, which are in many cases technical in nature. This suggests that restatements in the pre-SOX were more irregular in nature.

FAIR VALUE

More than 40 Statements of Financial Accounting Standards (SFASs) require or permit the use of fair value measures for assets and liabilities within GAAP. Methods for measuring fair value in these accounting standards prior to SFAS No. 157 were diverse and inconsistent. The changes to current accounting practices resulting from the adoption of SFAS No. 157 involve the definition of fair value, methods used to measure fair value, and the extended disclosures regarding fair value measurements. SFAS No. 157 defines fair value as the price that would be received to sell an asset or paid to transfer a liability at the measurement date in an ordinary transaction between market participants (buyers and sellers) at the principal or most advantageous market. The massive write-down that financial firms are recognizing and disclosing has begun to spur a backlash among corporate executives and investors who are basically blaming fair value measurements and rules for their incurred losses. The use of fair value accounting has been blamed for contributing to the recent financial crisis. Financial institutions and investors have contested the relevance, usefulness, and validity of fair value accounting standards.

STOCK OPTIONS ACCOUNTING

Stock option backdating is the practice of granting options that are dated prior to the actual grant date. This practice has raised several governance, legal, accounting, tax, and auditing concerns. Granting of discounted stock options to employees as well as improper recording and filing with the SEC is illegal. Under the SEC's 1992 rule, executives could legally delay reporting option grants for a long time, which made it difficult to determine whether options were being backdated. Under Section 409 A of the Internal Revenue Code, any backdated stock options are regarded as discounted stock options and are subject to additional taxes and penalties at vesting. It should also be noted that legal issues pertaining to backdating practices might occur when companies falsify documents submitted to regulators or investors in order to conceal their practices. In the post-SOX period, option grants to senior executives must be reported within two days of the grant dates, compared to at least 45 days in the pre-SOX period. This shorter reporting period is expected to substantially reduce the opportunity for management to engage in options backdating practices.

XBRL-GENERATED FINANCIAL REPORTS

XBRL enables computer systems to assemble data electronically in instance documents (documents that contain XBRL elements), retrieve data directly from XBRL instance documents, and convert data to human-readable financial reports. XBRL is expected to:

- Reduce substantially the manual effort involved in the preparation of financial statements
- Strengthen the ICFR
- Improve financial statement comparability
- Level the playing field for investors to gain access to real-time, online financial information

The SEC's intent is to improve the efficiency of capital markets by making financial information more suitable, less costly, and more timely. It is expected that the SEC, in the foreseeable future, will require the use of XBRL in reporting and filings. XBRL is based on an XML scheme, which is simply a "bar code" process that enables organizations to present their financial information in a format easily understood and processed by computers while being quickly transmitted internally and externally to investors, regulators, and analysts.

CONVERGENCE TO INTERNATIONAL FINANCIAL REPORTING STANDARDS

During the past several years, more than 100 countries have adopted International Financial Reporting Standards (IFRS) as accounting standards for their financial reporting purposes. It appears the momentum toward a single set of globally accepted accounting standards, such as U.S. GAAP, will ultimately be replaced by IFRS. Some challenges that need to be addressed to facilitate convergence toward IFRS are the following:

- Consistent interpretation and application of IFRS across jurisdictions
- Feasibility of adoption of IFRS by U.S. multinational companies, particularly U.S. companies
- Educating market participants regarding the differences between U.S. GAAP and IFRS
- Effects of switching from national accounting standards to IFRS for regulatory filing purposes and auditing

Convergence benefits include the following:

- Facilitating comparability of financial reports of companies in different countries and thus providing greater opportunity for investment and diversification

- Mitigating the risk that global investors may not fully understand the nuances of different national accounting policies and practices, which leads them to reach improper and potentially misleading conclusions from comparative analyses
- Enabling international audit firms to standardize their staff training and provide better audit quality worldwide
- Enhancing consistency and efficiency of global audit practices in addressing global accounting policies and practices and their potential deficiencies
- Mitigating the confusion associated with having to understand various reporting regimes

ANTIFRAUD APPLICATIONS FOR PRACTICE

ANTIFRAUD ENVIRONMENT

Antifraud controls are typically implemented by organizations to deter, prevent, and provide early fraud detection. Controls include:

- Establish an appropriate tone at the top
- Maintain an adequate and effective system of checks and balances
- Develop effective corporate governance
- Ensure a responsible and accountable board of directors
- Hire an objective and independent auditing firm
- Establish an independent whistle-blower system
- Maintain an independent and effective internal audit

These activities can be organized according to deterrence, prevention, and detection as shown in Exhibit 2.5.

TONE AT THE TOP AND WHISTLE-BLOWER HOTLINES

Tone at the top refers to the atmosphere that is created in the workplace by an organization's leadership. The theory is that management's tone will trickle down through the organization. If management acts ethically and with integrity, it is more likely that others in the organization will do the same. In addition, the tone at the top also creates an expectation and reflects the organization's overall culture. To set the tone, managers need to follow four steps:[10]

1. Communicate the organization's ethical expectations
2. Lead by example
3. Provide a safe mechanism for reporting violations
4. Reward integrity

Exhibit 2.5 Category Classification for the Fraud-Related Controls

Deterrence	Prevention	Detection
• Code of conduct • Internal audit/fraud examination department • Employee support programs • Management certification of the financial statements • Independent audit committee • Hotline • Fraud training for managers/executives • Fraud training for employees • Antifraud policy • Job rotation/mandatory vacation • Rewards for whistle-blowers	• Internal audit/fraud examination department • Hotline • Surprise audits • Rewards for whistle-blowers	• External audit of the financial statements • External audit of internal control over financial reporting • Management review of internal control

Source: Association of Certified Fraud Examiners, *2008 Report to the Nation on Occupational Fraud and Abuse;* available at www.acfe.com/documents/2008-rttn.pdf.

Some argue that fraud cannot be prevented; it can only be deterred. The simple explanation is that fraud cannot be prevented because it would be too costly to develop a system of checks and balances to prevent every type of fraud. There are too many potential schemes and fraudsters dedicated to their craft for the benefits of fraud prevention to exceed the associated costs. Generally, deterrence is centered on two concepts:

1. The perception and fear of getting caught
2. The perception and fear of disciplinary, criminal, and civil actions being taken against perpetrators

The tone at the top really is about more than perceptions; it is about creating a culture. Organizations begin the process with codes of conduct. Codes of conduct should be established and signed by the organization's key constituents:

- Members of the board of directors
- Executive management
- Managers and supervisors
- Employees
- Vendors
- Suppliers
- Contractors
- Consultants

In addition, the company's commitment to ethical behavior should also be communicated to customers. But having a code of conduct and getting stakeholders to sign it is just the beginning.

COMMUNICATE THE ORGANIZATION'S ETHICAL EXPECTATIONS

To create a culture of ethical behavior, the organization needs to communicate its commitment repeatedly and through a variety of mechanisms. The Institute of Internal Auditors (IIA), AICPA, and Association of Certified Fraud Examiners (ACFE) in ''Managing the Business Risk of Fraud: A Practical Guide'' suggest several methods of continuous communication and reinforcement:[11]

- Posters
- Flyers in paychecks, vendor payments, customer invoices
- Articles in company newsletters
- New releases—changes to program
- Antifraud training and awareness

LEAD BY EXAMPLE

A key characteristic of success is tied to making sure that every level of the organization lives, breathes, eats, drinks, and sleeps the tone at the top. ''Top'' is a relative descriptor. For the line employee, the top includes members of the board of directors, executive management, managers, and supervisors. Even the smallest of signals can work to erode the organization's culture. For example, some of the violations of traditional ethical behavior include:[12]

- Abusive or intimidating behavior of superiors toward employees
- Lying to employees, customers, vendors, or the public
- A situation that places manager interests over organizational interests
- Violations of safety regulations
- Misreporting actual time or hours worked
- E-mail and Internet abuse
- Discrimination on the basis of race, color, gender, age, or similar categories
- Stealing, theft, or related fraud
- Sexual harassment
- Sale of goods or services that fail to meet specifications
- Misuse of confidential information

- Price fixing
- Giving or accepting bribes, kickbacks, or inappropriate gifts

Clearly, while such a list is incomplete, such behavior should be avoided.

PROVIDE A SAFE MECHANISM FOR REPORTING VIOLATIONS: THE WHISTLE-BLOWER HOTLINE

The notoriety and recognition associated with such famous whistle-blowers as Cynthia Cooper of WorldCom, Sherron Watkins of Enron, and Coleen Rowley of the FBI, the 2002 *Time* magazine ''Persons of the Year,'' has led to greater understanding of the need for both blowing the whistle and protecting those with the courage to come forward to report inappropriate behavior.

The ACFE's 2008 *Report to the Nation on Occupational Fraud and Abuse*[13] indicates that 66 percent of frauds are discovered by tip or accident. Thus, a reporting mechanism needs to be developed and protected. Despite the attention given to whistle-blower hotlines, violation reporters will often come forward in a face-to-face manner. For example, according to The Network's ''Best Practices in Ethics Hotlines,'' nearly 50 percent of hotline callers give their name and roughly 33 percent indicate that they have previously informed management of the situation.[14] Thus, open-door policies and access to appropriately trained personnel in human resources, corporate counsel, senior management, executive management, the corporate compliance office, the audit committee, and security should all be options for reporting violations of company policies, procedures, and ethical standards.

Of course, one communication outlet needs to be an anonymous whistle-blower hotline. Some key attributes of the whistle-blower hotline include:[15]

- 24 hours-a-day/7 days-a-week (24/7) availability
- Trained and skilled interviewers
- Multilingual interviewers
- A means to deal with international tipsters whose culture and value system may differ from that at corporate headquarters
- A mechanism for the tipster to call the hotline again in the future to provide additional details and new information (e.g., unique number)
- Availability to report any type of improper behavior
- Real/genuine anonymity, if requested by the tipster
- No retaliation or retribution against those who report
- Appropriate and timely reaction to information

Many hotlines are staffed by outside professionals. No matter who provides the hotline, a protocol is required for who is to be notified. Finally, the attributes of the

hotline should be periodically tested by the internal audit group and the results reported to the board of directors.

REWARD INTEGRITY

The company, when it can, should reward those who highlight improper conduct. Tipsters, including employees, customers, vendors, and suppliers, can be given public recognition and accolades for their efforts, as well as monetary awards, when appropriate. Under no circumstances should whistle-blowers be retaliated against, directly or indirectly (e.g., prevented from receiving a future promotion by a disgruntled supervisor). Appropriate and timely investigation as well as resolution of the issues will often be reward enough for tipsters. Complaints should be tracked, and such tracking should include outcomes and final resolutions. And periodically, data related to the hotline should be communicated to the board of directors.

The last thought: We are often so dependent on people who are willing to do the right thing that we must ensure that we make doing the right thing easy.

NOTES

1. Peter C. Fusaro and Ross M. Miller, *What Went Wrong at Enron* (Hoboken, NJ: John Wiley & Sons, 2002).
2. Alan Reinstein and Thomas Weirich, ‘‘Accounting Issues at Enron,’’ *The CPA Journal* (December 2002); available at: http://www.nysscpa.org/cpajournal/2002/1202/features/f122002.htm.
3. David Barboza and John Schwartz, ‘‘Fastow: The Financial Wizard Tied to Enron’s Fall,’’ *New York Times*, November 5, 2002; Juan A. Lozano, ‘‘2 Enron Execs’ Sentences Reduced,’’ The Ledger.com (Associated Press), November 18, 2006.
4. K. Eichenwald and D. B. Henriques, ‘‘Enron’s Many Strands: The Company Unravels; Enron Buffed Image to a Shine Even as It Rotted from Within,’’ *New York Times*, February 10, 2002.
5. Much of information presented in this section comes from Zabihollah Rezaee, *Corporate Governance Post-Sarbanes-Oxley* (Hoboken, NJ: John Wiley & Sons, 2007).
6. Ibid.
7. FASB, *Statements of Financial Accounting Concepts: Accounting Standards 1999/2000 Edition* (New York: John Wiley & Sons, 1999).
8. FASB, *Statement of Financial Accounting Concepts No. 2: Qualitative Characteristics of Accounting Information* (New York: John Wiley & Sons, 1990).
9. J. Hranaiova and S. L. Byers, ‘‘Changes in the Market. Responses to Financial Restatements Announcements in the Sarbanes-Oxley Era,’’ Working paper 2007-001, PCAOB, October 11, 2007.

10. ACFE, ‘‘Tone at the Top: How Management Can Prevent Fraud in the Workplace,’’ undated.
11. ACFE ‘‘Managing a Business Risk of Fraud’’ a practical guide, June 2008; available at www.acfe.com/documents/managing-business-risk.pdf.
12. Developed from Ethics Surveys at www.ethicsworld.org and ACFE ‘‘Tone at the Top.’’
13. ACFE, *2008 Report to the Nation on the Occupational Fraud and Abuse*; available at www.acfe.com/documents/2008-rttn.pdf.
14. The Network, ‘‘Hotline Best Practices. A Framework to Create an Effective Anonymous Reporting Program,’’ 2004; available at www.reportline.net/news/downloads/TNW-GOVWP-CM.pdf.
15. Ibid.

Part Two

Financial Statement Fraud Profile, Taxonomy, and Schemes

Chapter 3

Cooking the Books Equals Fraud

INTRODUCTION

Financial statement fraud has received considerable attention from the public, press, investors, the financial community, and regulators because of high-profile, widespread fraud at big companies. Corporate executives were convicted of cooking the books and, in many cases, sentenced to jail terms. Recent business failures of financial firms such as AIG, Lehman Brothers, Merrill Lynch, Bear Stearns, Freddie Mac, and Fannie Mae have caused a market meltdown. Executives of these failed financial firms were generously compensated for making bad judgments and in some cases alleged fraudulent decisions. Taxpayers are paying for the unethical and incompetent activities of these firms. This meltdown affects everyone in society, as it has destroyed retirement funds, children's education funds, and other investments. This chapter presents profiles of several companies alleged and/or convicted by the Securities and Exchange Commission (SEC) of engaging in financial statement fraud, reviews these alleged financial statement fraud cases, and demonstrates that cooking the books causes financial statement fraud, which results in a crime. Indeed, the Sarbanes-Oxley Act of 2002 (SOX) increased both civil and criminal liability for corporate wrongdoers.

As a point, consider ZZZZ Best's Barry Minkow, the self-described General Motors of carpet cleaning. Barry Minkow grew up in the carpet cleaning business, assisting his mother starting at the age of 9. By 15, in 1981, he started his own carpet cleaning business, ZZZZ Best. By age 21, ZZZZ Best was a public company and Minkow was personally worth more than $100 million.[1] A major factor in taking the company public was the revenue and profits gained from converting the company from carpet cleaning to building restoration, allegedly for insurance proceeds. The problem with that premise, however, was that ZZZZ Best was not doing any insurance restorations. The revenues being reported for insurance restoration were completely fictitious and achieved through cooking the books.[2]

WHY DOES FINANCIAL STATEMENT FRAUD OCCUR?

Financial statement fraud occurs for a wide variety of reasons, including when motives combine with opportunity. Financial statement fraud may serve many purposes, including:

- Obtaining credit, long-term financing, or additional capital investment based on misleading financial statements
- Maintaining or creating favorable stock value
- Concealing deficiencies in performance
- Hiding improper business transactions (e.g., fictitious sales or misrepresented assets)
- Resolving temporary financial difficulties (e.g., insufficient cash flow, unfavorable business decisions, maintaining prestige)

Management may also engage in financial statement fraud to obtain the personal benefits of the following:

- Increased compensation through higher reported earnings
- Enhanced value of personal holding of company stock, such as stock-based compensation
- Converting the company's assets for personal use
- Obtaining a promotion or maintaining the current position within the company

Corporations' strategies to meet or exceed analysts' earnings forecasts pressure management to achieve earnings targets. Managers are motivated or, in most cases, rewarded when their bonuses are tied in to reported earnings, which can lead managers to choose accounting principles that may result in the misrepresentation of earnings. Companies are more likely to engage in financial statement fraud when:

- The selected accounting scheme is considered to be within a set of acceptable accounting alternatives.
- There is a strong motive to commit fraud.
- There is an opportunity to issue fraudulent financial statements.

Motive and opportunity may not play an important role if the fraud scheme is not viewed as an acceptable alternative.

PROFILE OF FINANCIAL STATEMENT FRAUD

Exhibit 3.1 summarizes a sample of the most recent high-profile financial statement fraud cases. Five interactive factors explain these high-profile financial statement frauds: cooks, recipes, incentives, monitoring, and end results. These factors can be abbreviated as CRIME. The right combination of these factors is a prerequisite for engaging in financial statement fraud. Exhibit 3.2 depicts these five interactive factors.

Exhibit 3.1 Sample of Financial Statement Fraud Cases

Company	Cooks	Recipe	Detection	Consequences
Enterasys	Eight former officers, including the chairman and the CFO	Artificially inflating revenue to increase, or maintain, the price stock	Some of the information came from former employees	• Shareholders lost about $1.3 billion • CFO was sentenced to 11 years in prison
Qwest Communications International, Inc	Two former top executives	Insider trading and exaggeration of sales	Whistle-blower letter from former employee	Joseph E. Nacchio, former CEO, was sentenced to six years in prison and paid a fine
BP America, Inc.	Former company traders	Trading manipulations	Prosecuted by DOJ's Criminal Division	• $100 million penalty • $125 million civil penalty to the CFTC
PNC ICLC Corporation	Company activities	Fraudulently transferring $762 million in mostly troubled loans and venture capital to off-balance sheet entities	Prosecuted by DOJ's Criminal Division	$115 million in restitution and penalties
AEP Energy Services, Inc.	Former company traders	Knowingly submitting false trading reports to market indices	Prosecuted by DOJ's Criminal Division	• $30 million criminal penalty • $21 million fine to the Federal Energy Regulatory Commission • Three energy traders also pled guilty
Superior Electric Company	President (owner) and CFO	Misappropriation of assets	Prosecuted by DOJ's Tax Division	• President sentenced to 34 months in prison and ordered to pay $4.8 million in restitution for the tax fraud scheme

(*continued*)

Exhibit 3.1 (*continued*)

Company	Cooks	Recipe	Detection	Consequences
				• CFO was sentenced to 15 months in prison and ordered to pay more than $1.62 million in restitution to the IRS
Thyssen, Inc.	Former CEO and executive vice president	Kickback schemes, filing false individual income tax returns	Prosecuted by DOJ's Tax Division	• Graham (CEO) sentenced to 75 months in prison and ordered to pay restitution of $8.8 million • Dresbach (executive VP) received 58 months in prison and fined $8.4 million in restitution • Allen (attorney and CPA) received 34 months in prison fined $8 million in restitution
UNI Engineering, Inc.	A former company controller	Obstructing the internal revenue laws	Prosecuted by DOJ's Tax Division	Controller was sentenced to 24 months in jail and ordered to pay a $7,800 fine
Neways, Inc.	Founders, former CFO, and corporate counsel	Concealing gross receipts, accounts	Prosecuted by DOJ's Tax Division	E. Mower (founder) was sentenced to 33 months in prison and ordered to pay a $75,000 fine
US Wireless	Former CEO and general counsel	Improperly transferring company stock and cash to offshore entities	Prosecuted by U.S. Attorney's Office for the Northern District of California	Hilsenrath (CEO) was sentenced to a five-year probation and ordered to pay $2 million in restitution

M&A West	A former corporate secretary	Securities fraud and five counts of money laundering	Prosecuted by U.S. Attorney's Office for the Northern District of California	Gilak (corporate secretary) was sentenced to 51 months' imprisonment and 36 months' supervised release
Mercury Finance Company	Former CEO, chairman of the board of directors, and CFO	Using accounting fraud scheme designed to inflate revenues and to understate its delinquencies	Prosecuted by U.S. Attorney's Office for the Northern District of Illinois	• Market capitalization of the company decreased by nearly $2 billion • Brincat (CEO) was sentenced to 10 years in prison
Anicom, Inc.	Former CEO, COO, controller, vice president of sales, and a shipping manager	Creating fictitious sales, understating expenses; overstating earnings	Prosecuted by U.S. Attorney's Office for the Northern District of Illinois	• Market capitalization loss of more than $80 million • All of the participants have pled guilty
Adelphia Communications Corp.	Former CEO and CFO	Participating in a complex financial statement fraud and embezzlement scheme	Prosecuted by U.S. Attorney's Office for the Southern District of New York	John (CEO) and Timothy Rigas (CFO) were sentenced to 15 and 20 years' imprisonment, respectively
Refco	Former top executives	Hiding massive losses sustained by the company in the late 1990s	Prosecuted by U.S. Attorney's Office for the Southern District of New York	• Public investor losses exceed $2 billion • It is in the trial process
ImClone Systems, Inc.	Former CEO of Martha Stewart Living Omnimedia and Merrill Lynch broker	Obstructing federal investigations into trading	Prosecuted by U.S. Attorney's Office for the Southern District of New York	• Martha Stewart sentenced to five months in prison and five months in home confinement

(*continued*)

Exhibit 3.1 (*continued*)

Company	Cooks	Recipe	Detection	Consequences
				• Peter Bacanovic (her broker) received five months in prison
CUC/Cendant Corporation	Two former executives together with their coconspirators	Improperly reversing merger reserves; delaying recognition of rejects-in-transit; engaging in early revenue recognition	Companies managers after the integration of CUC International and Parsippany and dismissed external auditors	• Shareholders lost more than $14 billion in market value • Shelton (former vice chairman) was sentenced to 120 months of imprisonment and to $3.275 billion in restitution • Forbes (former chairman) was sentenced to 151 months' imprisonment and $3.275 billion in restitution
HBO & Company	Two former executives, co-President, and co-chief operating officers	Inflating company revenues and earnings by hundreds of millions of dollars from 1997 through March 1999	Fraud was discovered by external auditor of combined McKesson HBO Company four months after McKesson Corporation Merged with HBO & Company	• One of the largest frauds, cost investors more than $9 billion • Share prices fell almost 50% in one day (from $65 to $32) • A former co-president of HBO & Co. agreed to pay $1.7 million to settle

				Securities and Exchange Commission charges • Co-chief agreed to pay a $1 million fine and about $733,000 in allegedly ill-gotten gains
Enron	Chairman, CEO, CFO	Overstating earnings, and equity through creation of Special Purpose Entities (SPE); inadequate disclosure of off-balance–sheet transactions (derivatives), and related financial activities	Media reports questioned the company's performance after departure of its chief executive officer and examination of its financial vehicles by federal regulators	• Loss of more than $80 billion in market capitalization • A former CEO of Enron sentenced to 292 months in prison • Enron's former CFO pled guilty and sentenced to six years in prison and its chief accounting officer received a sentence of five and one-half years
Warnaco Group, Inc.	Three top executives	Disseminating materially false and misleading statements	SEC enforcement officers	Price of each Warnaco share fluctuated from $5.97 on February 13, 2001, to close at $0.67 on April 18, 2001

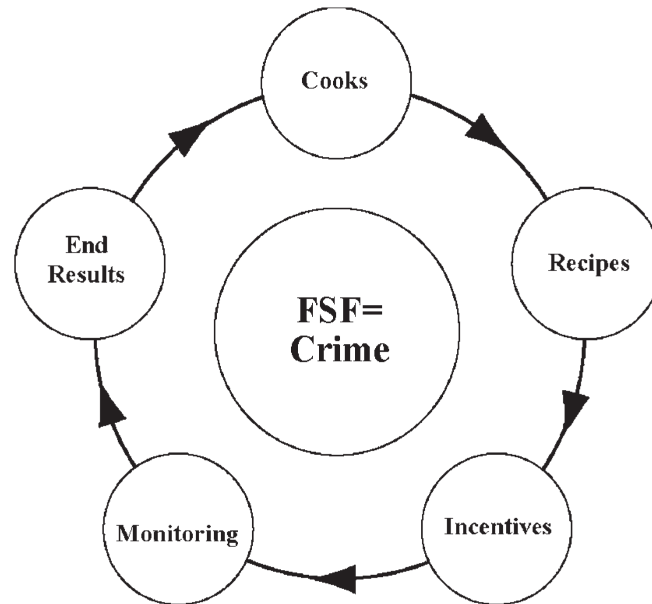


Exhibit 3.2 Financial Statement Fraud Interaction (Crime)

COOKS

The first letter in the word CRIME stands for cooks. The financial statement fraud cases presented in Exhibit 3.1 and the results of the 1999 "COSO Report on Fraudulent Financial Reporting" reveal that in most cases (more than 80 percent), the chief executive officers (CEOs) and/or chief financial officers (CFOs) were associated with financial statement fraud.[3] Almost all financial statement frauds occur with the participation, encouragement, approval, and knowledge of top management teams, including CEOs, CFOs, presidents, treasurers, and controllers. Other individuals typically involved with financial statement fraud are senior executives, board of director members, other senior vice presidents, and internal and external auditors.

Financial statement fraud has become the focus of public attention in recent years because of corporate wrongdoing in almost all industrial sectors. A consensus may be emerging that financial statement fraud is more often the result of actions or inactions, deliberate or inadvertent, by the top management team. This consensus has been used as the basis and rationale for holding company officials personally responsible for occurrences of financial statement fraud, liable for resulting losses, and subject to fines as well as potential incarceration.

Several provisions of SOX are intended to hold senior executives of public companies more accountable and responsible for producing reliable, accurate, and complete financial reports. These provisions require that:

- CEOs and CFOs certify the accuracy and completeness of financial reports.
- Management is responsible for the effectiveness of both design and operation of the internal controls over financial reporting.

- Management does not take any actions to fraudulently influence, coerce, manipulate, or mislead auditors in the conduct of their audits of financial statements.
- Management should reconcile pro forma statements with financial statements.
- Management's discussion and analysis (MD&A) sections should discuss and fully disclose critical accounting estimates and accounting policies.
- Top executives return any benefits they have received if it is proven that they misstated their company's financial reports filed with the SEC.
- Companies promptly disclose any insider stock trades.
- Companies ban loans to their senior executives and directors.

The proper implementation of these provisions of SOX is expected to influence the behavior of senior executives of public companies and encourage them to be more conscientious, conservative, and skeptical regarding their company's financial reports.

RECIPES

The second letter in the word CRIME stands for recipes. The fraud cases presented in Exhibit 3.1 and the findings of the 1999 "COSO Report on Fraudulent Financial Reporting" indicate that most financial statement fraud (about 90 percent) involved the manipulation, alteration, and falsification of reported financial information, with a small percentage (almost 10 percent) involving misappropriation of assets. Fraud schemes are many and often involve more than one technique to misstate financial statements. Overstating of revenues and assets causes most misstatements or financial statement frauds; about 20 percent involves understatements of liabilities and expenses. The 1999 COSO report reveals that more than half of the alleged fraud cases were perpetrated through overstating revenues by recording revenues prematurely or fictitiously. Fraudulent revenue schemes often used by companies are the following:

- Bill-and-hold sales transactions
- Side agreements revenue transaction
- Conditional sales
- Improper recognition of consignment sales as completed sales
- Unauthorized shipments
- Illegitimate cutoff of sales transactions at the end of the reporting period

These and other sham transactions will be thoroughly examined in Chapter 5. Financial statement frauds can range from overstating revenues and assets to understating liabilities and expenses, which typically begins with a misstatement of interim financial statements and continues into annual financial statements.

INCENTIVES

The third letter in the word CRIME stands for incentives and explains the most common motivations for companies and their cooks to perpetrate financial statement fraud. Economic incentives are typical in financial statement fraud cases, even though other motives—whether psychotic, egocentric, or ideological—can play a role. Fiscal pressure and the enticements to meet Wall Street's forecasts are the fundamental motives for publicly traded companies to engage in financial statement fraud.

Financial statement frauds typically are committed for a broad variety of reasons and are motivated by many factors. Prior research[4] has identified these reasons as the primary motivations for financial statement fraud:

- Meet company goals and objectives
- Comply with financing covenants
- Receive performance-related bonuses
- Obtain new financing or more favorable terms on existing financing
- Attract investment through the sale of stock
- Disclose unrealistic increased earnings per share
- Dispel negative market perception

Psychotic motivation is viewed in terms of a ''habitual criminal'' and is not common to financial statement fraud. The behaviors of those in corporate governance positions (e.g., management, top executives, and auditors) is scrutinized, and in most cases an individual with psychotic motivation would not hold his or her job for long. Egocentric motivations are any pressures to fraudulently achieve more personal prestige. This type of motive can be seen in people with aggressive-type behavior who desire to achieve higher functional authority in the corporation. Ideological motivations occur when individuals are encouraged to think that their behavior or cause is morally superior. It can be seen in aggressive top executives who attempt to be market leaders or improve their market position in the industry. The economic motive of meeting analysts' forecasts and making Wall Street happy, coupled with egocentric and ideological motives, is the primary cause of financial statement fraud. Of course, one challenge faced by those attempting to identify fraudulent activity is that the personal characteristics of fraudsters often mirror those expected in successful CEOs, entrepreneurs, and other business professionals.

Incentives provide motivation to engage in financial statement fraud. Agency theory, which defines the relationship between principles (owners) and agents (managers), suggests that the presence of conflicts of interest between the top management team and shareholders and creditors adversely affects the quality and integrity of the financial reporting process and increases the probability of financial statement fraud. Empirical studies[5] identify two fundamental

variables—management stock ownership and proximity to debt covenant limits—that affect management's propensity to engage in financial statement fraud. These studies suggest goal congruence between management and shareholders in the 0 to 5 percent and in the above-25 percent ranges of management stock ownership. However, in the range of 5 to 25 percent, the opportunistic behavior by management is anticipated, and thus the probability of financial statement fraud increases.

MONITORING

The fourth letter in the word CRIME stands for monitoring. Responsible corporate governance that sets the tone at the top by demanding high-quality financial reporting and not tolerating misstated financial statements is the most important proactive monitoring mechanism for preventing and detecting financial statement fraud. The second most important monitoring mechanism is the presence of adequate and effective internal control structure. Although management is primarily responsible for designing and maintaining internal controls, the audit committee, internal auditors, and external auditors should ensure that internal controls are adequate and effective in preventing, detecting, and correcting financial statement fraud and should eliminate, as much as possible, room for management to override control activities. The audit committee can play an important role in overseeing the integrity and quality of the financial reporting process and the effectiveness of the internal control structure. Companies should view the audit committee as a value-added oversight function and not merely a window-dressing position to satisfy the new requirements of the SEC, New York Stock Exchange (NYSE), and National Association of Securities Dealers (NASD) for audit committees.

The importance of effective internal and external audit functions in preventing and detecting financial statement fraud is supported in the business literature and authoritative standards and reports (Treadway reports, AICPA's SAS no. 99). Internal auditors are viewed as the first defensive line against financial statement fraud. External auditors traditionally have been held accountable for detecting financial statement fraud. Companies should hire tough external auditors who help them prevent and detect financial statement fraud rather than those that rubber-stamp management assertions to collect fees for auditing and other consulting services. The financial reporting process of publicly traded companies must include a monitoring mechanism. The monitoring mechanism consists of the direct oversight function of the board of directors, the audit committee, external auditors, and regulatory agencies; and the indirect oversight function by those who follow the company in the role of owner/investor as an intermediary, such as analysts, institutional investors, and investment bankers. Corporate gatekeepers, including directors, auditors, and legal counsel, are responsible for enforcing these monitoring mechanisms. Monitoring can create an environment that reduces the likelihood of financial statement fraud. The extent

of monitoring in the financial reporting process should be negatively correlated with the probability of occurrence of financial statement fraud. The board of directors and its representative audit committees are responsible for overseeing the integrity and quality of the financial reporting process in providing reliable, relevant, and useful financial statements.

END RESULTS

The last letter in the word CRIME stands for end results. The consequences associated with financial statement fraud can be severe. Adversarial consequences typically range from filing for Chapter 11 bankruptcy (36 percent of alleged fraud) to changing owners (15 percent), delisting by the national stock exchange (21 percent), and substantial decline in stock value (58 percent). Top executives involved in cooking the books often suffer personal consequences of:

- Losing the value of their stock-based compensation
- Being forced to resign or being fired (about 30 percent of top executives)
- Being barred by the SEC from serving as officers or directors of another publicly traded company
- Being sanctioned for fines or jail terms

Independent auditors involved in financial statement fraud also often suffer personal and professional consequences. For example, in the case of Waste Management financial statement fraud, four of the partners of Arthur Andersen associated with the company's audit were barred from practicing before the SEC for some time period ranging from one year to five years, and they paid $120,000 in civil fines. In addition, Arthur Andersen was fined $7 million for signing off on a financial statement for Waste Management that inflated its earnings by more than $1 billion over four years.

Reported incidents of financial statement fraud (Enron, WorldCom) prove that firms engaged in and/or convicted of financial statement fraud typically pay high consequences for their illegal actions because their legitimacy is challenged and their financing activities in obtaining resources are more difficult and costly and often go bankrupt. It is estimated that the recent subprime mortgage crisis and the resulting global economic meltdown caused by corporate irregularities cost more than $1.5 trillion. Given the high cost associated with financial statement fraud and even by unsuccessful fraudulent financial reporting activities, the decision by corporations to engage in such activities must be justified by strong motives that compel firms to behave illegally.

SOX has provided more severe criminal and civil penalties for corporate wrongdoers and those who violate securities laws, penalties that are intended to protect investors. Corporate government reforms, including SOX, established in response to the rash of financial scandals at the turn of the twenty-first century, have caused

a cultural change in corporate America in regard to mitigating corporate malfeasance and accounting fraud. Investors, particularly institutional investors, are more engaged and empowered to influence boardroom behavior and actions through their proxy statements. Lawmakers and regulators are more sensitive to the needs of investors and liable to bring enforcement actions against corporate wrongdoers. The ‘‘new world order’’ of increasing scrutiny by investors and the corporate board has created a healthier culture of managing the company for sustainable performance and long-term growth rather than managing the numbers and cooking the books for short-term gain. Corporate greed and dubious accounting schemes are not necessarily criminal; prosecutors must demonstrate that corporate wrongdoing and violation of laws were conducted with the intent to mislead and harm investors.

FBI Arrests Two for Hedge Fund Investment Fraud

Paul Greenwood and Stephen Walsh were arrested in late February 2009 for allegedly perpetrating a $553 million hedge fund fraud, one of the largest hedge fund frauds on record. The amount of the fraud, $553 million, represented approximately 83 percent of the $668 million collected from investors, primarily institutional clients. The fraud was discovered through the auditing efforts of the National Futures Association (NFA). Because the NFA auditors concluded that Greenwood and Walsh did not cooperate and produce books as well as records, it had suspended the men from NFA membership and prohibited them from soliciting new investments.

According to the SEC civil complaint, Greenwood and Walsh used their clients’ funds for their personal piggy bank to furnish lavish and luxurious lifestyles, which included the purchase of multimillion-dollar homes, a horse farm, cars, show horses, and collectibles, including rare books and Steiff teddy bears. The Commodities Futures Trading Commission concluded that the two had spent more than $160 million for their personal expenses.

Like the Madoff and Stanford Financial frauds discussed earlier, the sophistication of the victims is frightening:

- Carnegie Mellon University had invested more than $49 million.
- University of Pittsburgh, more than $65 million.
- Iowa Public Employees Retirement System, approximately $339 million.
- Sacramento County Employee’s Retirement System, approximately $89.9 million.

Greenwood and Walsh, through their company WG Trading, promised to invest the money in something called ‘‘enhanced stock indexing.’’ From January 1995 to September 2008, WG Trading never reported a loss in any month. Typically, gains ranged from 0.10 percent to 1 percent per month.

The alleged perpetrators face civil and criminal charges including conspiracy, securities, and wire fraud.

Source: Steve Stecklow, Chad Bray, and Jenny Strasburg, ‘‘Pair Lived Large on Fraud, U.S. Says,’’ *Wall Street Journal*, February 26, 2009.

WASTE MANAGEMENT, INC.: FINANCIAL STATEMENT FRAUD ANALYSIS

In this section, a real financial statement fraud case is analyzed in light of the five interactive fraud factors: cooks, recipes, incentives, monitoring, and end results (CRIME), as depicted in Exhibit 3.3. This landmark 1990s fraud case was:

- The largest-ever civil penalty against a company, in this case Arthur Andersen, formerly one of the ''Big Five,'' accounting firms
- The first antifraud injunction in more than 20 years
- The largest restatement of fraudulent earnings reported by a company in U.S. history

This case involving allegations of financial statement fraud originally drew analysts' attention in 1997 when the company's CEO quit after three months. Analysts concluded that the departed CEO might have discovered accounting problems. The SEC began examining Waste Management's books in November 1997, when the company announced that a change in accounting methods would result in a $1.2 billion loss and reduce the reported retained earnings of $1 billion that was recorded over the previous five years. Arthur Andersen had been auditing Waste Management Services since 1971, before the garbage removal company went public. In 1992, auditors at Andersen found evidence suggesting that their client misstated taxes, insurance, and deferred costs by $93.5 million, but Waste Management refused to restate financial statements to correct the mistake. In 1993, the auditors documented another $128 million misstatement that would have reduced income from continuing operations by 12 percent. Nevertheless, Andersen concluded that the misstatement was not material to require disclosure. In 1995, the auditors considered another $160 million misstatement to be immaterial and thus not warranting disclosure on the financial statements. Between 1992 and 1996, Waste Management continued to engage in $1.4 billion in financial statement fraud.

The important lesson to be learned from this landmark accounting and auditing fraud case is financial statement fraud equals CRIME. The *c*ooks were the top management team, including the chief financial officer and chief accounting officer, at Waste Management who were in collusion with four partners of

Exhibit 3.3 Financial Statement Fraud Formula

Cooks	+
Recipes	+
Incentives	+
Monitoring (lack of)	+
End Results	=
CRIME	

Andersen. The *r*ecipe was overstatement of earnings and hidden expenses for five years, causing misstatements in the published audit financial statements. There were several *i*ncentives for the client and auditors to engage in financial statement fraud:

- Management experienced pressures to meet earnings' expectations and make Wall Street happy.
- Auditors were also under pressure to retain their clients at the expense of compromising their ethical conduct and professional responsibilities.
- Andersen considered Waste Management a ''crown jewel'' client and failed to stand up to management pressure to disclose discovered misstatements in the financial statements for several years.

Apparent conflicts of interest between the top management team of Waste Management and auditors of Andersen also existed:

- Every chief financial officer and chief accounting officer in Waste Management's history had previously worked as an auditor at Andersen.
- Over several years, Andersen billed Waste Management more fees for management advisory services than for auditing services ($11.8 million for other services compared to $7.5 million for auditing).
- An Andersen affiliate billed Waste Management an additional $6 million for consulting services.
- The compensation of Andersen's lead partner on the Waste Management audits was based in part on the amount of money Andersen billed Waste Management for nonaudit services.

*M*onitoring in this fraud scheme formula refers to the lack of existence of responsible corporate governance in monitoring management functions for fair presentation of financial statements in conformity with GAAP. The absence of oversight function by the audit committee of Waste Management, coupled with ineffective monitoring of the top management team by the board of directors and an inadequate and ineffective internal control structure in preventing, detecting, and correcting financial statement fraud, might have been significant contributing factors to the misstatements and audit failures.

The *e*nd result of the financial statement fraud committed by Waste Management resulted in these outcomes:

- A shareholder class action in Chicago cost the company and its auditor, Andersen, a combined total of $220 million, where Andersen paid $75 million.
- Waste Management took a total of $3.54 billion in charges and write-downs in 1997 when the fraudulent accounting practices were initially uncovered.

- Stock prices of Waste Management fell down substantially upon discovery and announcement of financial statement fraud.
- The top management team at Waste Management, including the chief financial officer and the chief accounting officer, were forced to resign.
- A settlement agreement was filed in a lawsuit pending in a Boston federal court.
- The SEC has issued rules in implementing provisions of SOX in levying restrictions on the consulting services that can be offered to audit clients.
- The auditors at Andersen were charged with ''knowingly and recklessly'' issuing false and misleading audit reports for several years.
- The auditors consented to an injunction of fraud, the first antifraud injunction in more than 20 years against a Big Five accounting firm.
- One former and three current partners of Andersen were barred for several years from auditing a U.S. publicly traded company.
- Andersen paid a record $7 million fine, which is the largest ever civil penalty against a Big Five accounting firm.
- Three of Andersen's Chicago-based current and former partners were fined a total of $120,000 in a civil lawsuit.

ANTIFRAUD APPLICATIONS FOR PRACTICE

ORGANIZATIONAL SELF-ASSESSMENT

The pervasiveness of financial statement fraud by high-profile corporations encourages public companies to take proactive roles by establishing strategies to prevent and detect such fraud. Corporate fraud prevention and detection strategies should be developed to foster the quality, integrity, and reliability of the financial reporting process. These strategies should include:

- *Targeted fraud risk assessment*. Fraud risk assessment should be performed both periodically and continuously. Corporations should consider and implement fraud vulnerability reviews based on their industry, competitive environment, and operational characteristics. Furthermore, corporations should establish whistle-blowing opportunities and use proactive forensic accounting techniques to detect and investigate financial statement fraud allegations.
- *Gamesmanship review*. A gamesmanship review is a comprehensive assessment of a top management team's philosophies, attitudes, operating styles, decisions, actions, beliefs, and ethical values pertaining to the financial reporting process. It is also a continuous review of management's financial reporting relationships with security analysts, internal auditors, external auditors, the board of directors, and the audit committee. A periodic gamesmanship review can improve

the quality of financial reporting by preventing and reducing the possibility of collusion between financial statement fraud perpetrators. Gamesmanship and its influence on the risk of financial statement fraud are more carefully examined in Chapter 9.

- *Fraud prevention program*. Corporations should develop fraud prevention programs; establish appropriate policies and procedures; communicate fraud policies and procedures to everyone within the corporation; enforce compliance with the policies; and periodically assess their effectiveness in preventing and detecting financial statement fraud.
- *Enforcement procedures*. The SEC stated that combating financial statement fraud by publicly traded companies is its first priority. Nonetheless, the SEC has been criticized for its inefficacy in the early discovery of recent financial statement fraud with respect to Madoff, Satyam, and Stanford Financial.

UNDERSTANDING THE LAW, FRAUD EXAMINATION, AND FINANCIAL FORENSICS

Fraud may be prosecuted criminally or civilly. Further, almost any dispute between parties such as individuals, businesses, organizations, and government entities can be pursued in civil court. Anytime the legal issue involves claims of fraudulent activity, fraud examiners and forensic accountants can play an important role in investigating and resolving those issues. Legal issues that involve ''money'' disputes provide an opportunity to engage qualified financial forensic professionals. What this means is that persons charged with responsibility to detect, investigate, and resolve financial transgressions as well as disputes need to understand something about the legal environment. While legal questions should be deferred to counsel, understanding the landscape is helpful. The primary areas include:

- Basic definition of financial forensics
- The rights of individuals
- Probable cause
- Rules of evidence
- Common legal infractions other than fraud

Because each of these topics is extensive, this presentation will touch on only the basics.

Basic Definition of Financial Forensics

In the most basic sense, financial forensics is the intersection between the law and an area that involves financial expertise: Accounting, economics, and finance are

the most common, but issues can also involve marketing, information systems, and management. Under common law, fraud includes four essential elements:

1. A material false statement (an act)
2. Knowledge that the statement was false when it was spoken (intent and concealment)
3. Reliance on the false statement by the victim (intent and concealment)
4. Damages resulting from the victim's reliance on the false statement (conversion or benefit in favor of the perpetrator)

Rights of Individuals

Generally, individuals have far fewer rights as employees than as citizens. For example, as an employee, an individual has an obligation to cooperate with the employer or be subject to dismissal. Other rights may be granted to employees as set out in employment contracts and collective bargaining agreements.

Interviews An employee's or suspected individual's right to avoid self-incrimination applies to employers, investigators, and law enforcement personnel. However, an employee who refuses to cooperate during an interview while invoking the Fifth Amendment may be subject to termination. A second issue arises with interviewees with regard to the Sixth Amendment, where employees are entitled to counsel. As long as a nonpublic entity is conducting the interview, an employee does not have the right to have a lawyer present, nor does the employee have the right consult an attorney prior to an interview. However, the employee maintains the right to consult an attorney if he or she requests to do so.

Searches The Fourth Amendment protects individuals against unreasonable searches and seizures. Unreasonable searches and seizures are forbidden. A workplace search is considered reasonable under two circumstances:

1. The search must be justified at its inception because it is likely to reveal evidence of work-related misconduct. The requirement implies that a clear suspicion exists based on a preliminary review of the evidence.
2. The search is necessary to further the investigation. An example of this concept is that the investigator will be able to obtain files that are a required part of the investigation. The requirement implies that the search is likely to reveal information pertinent to the investigation.

Assuming that the search is reasonable, based on these criteria, the scope of the search must be no broader than is necessary to serve the organization's legitimate, work-related purpose. The investigator may in fact have no search limitations if the employee has no reasonable expectation of privacy in the place to be searched.

Surveillance Surveillance techniques include electronic surveillance and audio and video monitoring and recording. Surveillance is trickier than interviews and searches. For this reason, counsel should be consulted when surveillance is contemplated.

Discharging a Suspected Wrongdoer from Employment It is advisable that employers document ''good cause'' for any termination in the employee's personnel file. Some considerations of good cause are:

- The employee's conduct was against written policy.
- The employee's conduct made for unsafe or inefficient business operations.
- The company completed a reasonable investigation to ensure that the nefarious act was committed by the employee and has evidence to support such a claim.
- The investigation was fair as well as objective and evidence suggested the elimination of alternative suspects.
- The termination was nondiscriminatory, meaning that all persons committing such an act were or would be subject to the same punishment (e.g., termination).
- The ''punishment fits the crime,'' meaning that the punishment is reasonable given the nature of the offense.

Probable Cause

Probable cause is the standard by which law enforcement may make an arrest, conduct a personal or property search, or obtain a warrant. The term also refers to the standard used by grand juries when they believe that a crime has been committed. The Fourth Amendment states that ''the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'' Despite this phraseology, the threshold for probable cause is not as high as one might expect. The challenge and where probable cause comes into play is the issue of how to obtain the necessary documents (i.e., physical documentary evidence). Generally, investigators can obtain documents using three approaches: voluntary consent, subpoena, and search warrant.

With voluntary consent or with a subpoena, the investigator relies on the subpoena recipient to determine which documents fall under the subpoena's particular details. In contrast, a warrant allows the holder of the warrant (and not the suspect and his or her defense counsel) to decide which documents are relevant and must be produced.

Rules of Evidence

Without evidence, there is no proof; without proof, there are no convictions. In the world of fraud and forensic accounting, truth needs to be grounded in evidence. Evidence-based decision making is paramount. Evidence is anything legally presented at trial to prove a contention and that can convince a jury. It is anything that

can be perceived by the five senses: sight, hearing, taste, touch, and smell. Further, in order to be presented, the evidence must be relevant, meaning that it tends to impact the beliefs of the persons to which it is presented.

Rules of evidence also deal with the problem of chain of custody. *Chain of custody* refers to those individuals who had possession of the evidence in question and what they have done with it. Essentially, fraud professionals and forensic accountants must be able to establish the origins of evidence and that it has not been altered as a result of the investigation or through possible corruption because the investigators have lost control of it. Close monitoring of all physical evidence is important in a fraud investigation.

Common Legal Infractions Other than Fraud

In the Qwest case, despite alleged fraudulent conduct, CEO Nacchio was not convicted of fraud but of insider trading. Martha Stewart and Arthur Andersen were convicted on obstruction of justice charges. Federal and state prosecutors will pursue those infractions of the law that are best supported by the evidence and can be explained to and understood by juries. Besides fraud, insider trading, and obstruction of justice, some of the other laws that prosecutors often pursue include:

- Mail fraud
- Wire fraud
- Tax fraud
- Securities fraud
- Money laundering
- Conspiracy
- Racketeering Influence and Corrupt Organizations Act (RICO)
- USA Patriot Act
- Bank Secrecy Act
- Sarbanes-Oxley Act

The last thought:

> *In civilized life, law floats in a sea of ethics.*
>
> —Supreme Court Chief Justice Earl Warren

NOTES

1. Jeff B. Copeland with Michael A. Lerner, “A Whiz Kid Goes Wrong,” *Newsweek*, July 20, 1987.
2. Alex Johanns, “Barry Minkow and the ZZZZ Best Fraud,” ACFE (Fall 2005).

3. M. S. Beasley, J. V. Carcello, and D. R. Hermanson, *Fraudulent Financial Reporting: 1987–1997: An Analysis of Public Companies* (New York: COSO, 1999).
4. Robertson J. C. *Fraud Examination for Managers and Auditors* (Austin, TX: Viesca Books, 2000).
5. R. Carter and R. Stover, ''Management Ownership and Firm Value Compensation Policy: Evidence from Converting Savings and Loan Associations,'' *Financial Management* (Winter 1991): 80–90. C. Latham and F. Jacobs, ''Monitoring and Incentives Factors Influencing Misleading Disclosures,'' *Journal of Managerial Issues* (Summer 2000): 169–187.

Chapter 4

Realization, Prevention, and Detection

INTRODUCTION

With the financial markets still struggling with the loss of confidence partially due to the Madoff fraud, market participants were again shocked in February 2009 when federal authorities charged R. Allen Stanford with carrying out a "massive, ongoing fraud" involving the sale of $8 billion in certificates of deposit (CDs). The size, breadth, and supposed sophistication of the fraud victims of the Madoff and Stanford frauds have continued to rattle the investing public. Like Madoff, Stanford Financial promised "improbable, if not impossible" returns to investors, often percentage points higher than those offered by rivals. Rather than true CDs, the Securities and Exchange Commission (SEC) alleged that the funds were invested in risky real estate and private equity holdings.[1]

This chapter presents a model consisting of conditions, corporate structure, and choice (3Cs) to explain and analyze motivations, opportunities, and rationalizations for financial statement fraud such as the one at Qwest and at Stanford Financial. The wrong combination of these three factors increases the likelihood of financial statement fraud. This chapter also focuses on the economic—external antecedent and internal antecedent—factors involved in financial statement fraud. Top management team characteristics, as well as financial statement fraud prevention, detection, and correction strategies, are also examined.

REALIZATION

The 2008 report of the Association of Certified Fraud Examiners reveals how fraud is commonly detected, including the role of the audit committee and internal and external auditors in discovering financial statement fraud.[2] It highlights the need for the audit committee to establish and maintain objective and independent whistleblowing policies and procedures; and for the external auditors to conduct surprise or unexpected audits of their clients. The report indicates that among the 237 cases of fraud resulting in a loss of $81 million or more, 16 percent were detected by external auditors, whereas 42 percent were discovered through a tip or a complaint. Frauds in small businesses were often uncovered through tips by internal auditors

and most likely by accident. These results suggest that antifraud policies and programs can play an important role in preventing and detecting fraud. There is evidence that the general public is becoming increasingly aware of financial statement fraud committed by publicly traded companies. An extensive review of actual financial statement fraud cases suggests that financial statement fraud will occur if:

- Favorable conditions for financial statement fraud exist.
- The corporate culture provides opportunities and motivations for the top management team to commit financial statement fraud (e.g., economic gain).
- The top management team can choose from among a set of accounting principles and practices the one that rationalizes its decision to engage in financial statement fraud.[3]

THE 3CS MODEL

This book uses a model consisting of conditions, corporate culture, and choice (3Cs) in explaining motivations (perceived pressures), opportunities, and rationalizations for financial statement fraud. Financial statement fraud may be perpetrated when the 3Cs are present. Such fraud may be committed for several reasons, all of which fall under these three categories.

This chapter examines a fraud scheme focusing on the 3Cs—conditions, corporate culture, and choice—to explain preexisting financial statement fraud causes and to predict as well as to discover potential financial statement fraud. Although the presence of a single factor can signal the possibility of fraud, the combination of two or more factors at any one time increases the likelihood that fraud might have occurred. If any of the three factors is missing, then the probability of financial statement fraud is diminished.

CONDITIONS

Financial statement fraud will occur if and when the benefits to the fraudster(s) outweigh the associated costs calculated using the probability and consequences of detection. Within this framework, financial statement fraud will occur especially in the following situations:

- Economic pressure resulting from a continuous deterioration of earnings
- A downturn in organizational performance
- A continuous decline in industry performance
- A general economic recession

Economic motives are common in financial statement fraud, even though other types of motives, such as psychotic, egocentric, or ideological motives (discussed in Chapter 3), can also play a role.

Pressure on a corporation to meet analysts' earnings estimates can be a factor stimulating earnings management and resulting in financial statement fraud. Earnings management seems to be a tactical response to a perceived need to meet earnings expectations. Management evaluates the benefit of earnings management in terms of the positive effect it will have on the company's stock price or the cost saving of preventing the negative impact on share prices for not meeting earnings forecasts against the possible cost of consequences of engaging in financial statement fraud and the probability of detection, prosecution, and sanction. Executive compensation typically is linked to short-term market performance rather than sustainable long-term performance, which provides adequate incentives for management to engage in earnings manipulation. The Corporate Library analyzed the link between executive compensation and company performance. It found that many public companies paid their top executives some of the highest salaries in 2006 while long-term shareholder value significantly decreased.[4] This finding suggests that there is no meaningful relationship between executive compensation and company performance.

Financial statement fraud is likely to increase when the perpetrator has the opportunity and the motive to engage in fraudulent financial activities. Financial statement fraud may occur for various reasons. In most instances, these reasons deal with the existence of opportunities to commit financial statement fraud. These conditions help to explain some of the impetus behind financial statement fraud:

- Lack of responsible corporate governance
- Ineffective board of directors
- Nonexistent or ineffective audit committee
- Dominant top management team with little or no accountability
- No review of top executives' activities and no requirements for executive disclosures
- Existence of related-party transactions and lack of oversight over transparency of those transactions
- Inadequate and ineffective internal audit functions
- Frequent changes in external auditors or selection of inexperienced external auditors
- Inability to obtain credit
- Unfavorable economic conditions
- Insufficient cash flows to support the reported earnings growth
- Restrictive loan agreements
- Excessive bad debt expenses resulting from inability to collect receivables
- Excessive investment and/or losses
- Dependence on only a few customers

CORPORATE CULTURE

Because financial statement fraud is typically committed at the level of the top management team rather than lower management or employees, one would expect incidences to occur most often in an environment characterized by ineffective corporate governance. Management would be more reluctant to engage in financial statement fraud when an effective corporate governance mechanism increases the probability of prevention and detection. Monitoring and oversight functions of corporate governance, including that involving the board of directors and the audit committee, are thoroughly examined in Chapter 6. Corporate governance refers to the way a corporation is governed through proper accountability for managerial and financial performance. The characteristics and attributes of corporate governance that are most likely to be associated with financial statement fraud are aggressiveness, cohesiveness, loyalty, opportunism, trust, and control effectiveness. Aggressiveness and opportunism can be shown by the company's attitude and motivations toward beating analysts' forecasts about quarterly earnings or annual earnings per share and the attempt to make Wall Street happy by reporting unjustifiable favorable financial performance. Cohesiveness and loyalty attributes create an environment that reduces the likelihood of whistle-blowing and increases the probability of cover-up attempts. Trust and control ineffectiveness can cause those in an oversight function (e.g., board of directors, audit committee) as well as assurance function (e.g., internal auditors, external auditors) to be less effective in detecting fraud. The cohesiveness can cause a sharply defined group boundary of corporate governance that creates high cooperation among corporate governance members to conceal financial statement fraud and impose greater restriction of fraudulent financial information to leak to outsiders. This cohesiveness can encourage more collusion in the development of financial statement fraud. If the fraud is discovered by internal or external auditors, it also motivates a push for a cover-up. When the members of corporate governance establish trust, it creates less room for suspicion and skepticism, which, in turn, may reduce the likelihood of auditors' detection of fraud.

Recent corporate governance reforms, including the Sarbanes-Oxley Act (SOX), SEC rules, listing standards, and best practices, have shifted the power balance among the company's shareholders, directors, and management. Shareholders have been more proactive in monitoring and scrutinizing their corporations and thus have heightened their expectations for directors' performance on their behalf. Directors have strengthened their commitment and accountability in fulfilling their fiduciary duties by overseeing management's strategic plans, decisions, and performance while spending more time on their duties, particularly in overseeing the financial reporting process. Management has stepped up its efforts to achieve sustainable shareholder value creation and enhancement, improving the reliability of financial reports through executive certification of internal controls and improving financial statements. The improved compliance with appropriate laws, rules, and regulations can create a sound corporate culture of establishing the right tone at the top that promotes ethical and responsible conduct throughout the company. A proper corporate culture requires the development of proper programs, policies,

and procedures to comply effectively with applicable laws, regulations, standards, and best practices. However, compliance just for the sake of compliance and the promotion of a check-box mentality is not enough. Corporations should establish an ethical culture that demands all corporate governance participants to do the right thing and refrain from conflicts of interest and fraudulent activities.

CHOICE

Management can use its discretion to choose between the shortcut alternative of engaging in illegal earnings management or ethical strategies of continuous improvements of both quality and quantity of earnings. Specifically, when neither environmental pressure nor corporate culture is a significant influence, financial statement fraud could occur simply as one of management's strategic tools or discretions motivated by aggressiveness, lack of moral principles, or misguided creativity or innovation. Under these circumstances, financial statement fraud is a matter of choice, regardless of environmental pressure, need, or corporate culture.

Perpetrators of financial statement fraud may be motivated to commit the fraud regardless of consequences of their actions or whether the sanctions exist. A company may, in good faith, view its regulations and requirements as too harsh and, to diminish their adverse impacts, may engage in financial statement fraud.

The three variables of conditions of pressure or need, corporate culture, and choices may each function separately, or perhaps more likely in combination in terms of their contribution to financial statement fraud. The wrong combination of these variables is a perfect recipe for financial statement fraud, as depicted in Exhibit 4.1.

Qwest: A Failure to Disclose?

Qwest is a leading provider of voice, video, and data services across America and the world. Homes and businesses around the globe rely on the company's dial-tone connection.[5] On March 15, 2005, the SEC charged Joseph P. Nacchio, former co-chairman and chief executive officer, and eight other former Qwest officers and employees with fraud and other violations of the federal securities laws. The SEC alleged that, between 1999 and 2002, the Qwest defendants engaged in a multifaceted fraudulent scheme designed to mislead the investing public about the company's revenue and growth. Nacchio and others traded Qwest stock knowing that the public disclosures were inconsistent with their private information. Prior to the SEC investigative findings, on July 29, 2002, Qwest admitted it had used improper accounting methods that boosted its profits by more than $1 billion during a three-year period. The company admitted to prematurely recording hundreds of millions of dollars of revenue at the end of its quarterly reporting periods. However, Qwest insisted that the ''accounting errors'' were made under policies approved by auditor Arthur Andersen.

Qwest projected overly aggressive estimates of revenue and earnings and used ''smoke and mirrors'' to meet those unrealistic projections. More specifically, the SEC alleged these acts:

- The perpetrators characterized nonrecurring revenue from one-time sales of capacity (indefeasible rights of use, or IRUs) and equipment as recurring ''data and Internet service revenues,'' using the fraudulent revenue to meet projections.

- Qwest provided secret side agreements to IRU customers, allowing those customers to exchange the capacity purchased for different capacity. The secret side agreements effectively concealed the true nature of the contracts from Qwest's accountants and auditors.
- Executives backdated IRU agreements so that the revenue could be recognized in earlier quarters than permitted by generally accepted accounting principles (GAAP).
- Qwest also concealed its actions by disclosing misleading information to the SEC and the public concerning the true nature of the transactions, the true underlying financial performance reflected in the income statement, and its related impact on the company's financial condition (balance sheet).

On April 19, 2007, Joseph Nacchio was found guilty—not on perpetrating a fraud scheme but on 19 counts of ''insider trading'' associated with his sale of $100 million of Qwest stock. In fact, prosecutors had been banned from telling jurors that Qwest had restated revenues to the tune of $2.48 billion in 2000 and 2001. On July 29, 2007, Nacchio was fined $19 million, forced to forfeit $52 million in stock profits that he was convicted of illegally acquiring, and sentenced to 6 years in prison. Nacchio was 57 at the time.

Sources: ''SEC Charges Former Qwest CEO Joseph Nacchio and Eight Others with Massive Financial Disclosure Fraud,'' March 15, 2005, from SEC ''For Immediate Release 2005-36''. Dionne Searchey, Peter Lattman, Peter Grant, and Amol Sharma, ''Qwest's Nacchio Is Found Guilty in Trading Case,'' *Wall Street Journal*, April 20, 2007. David W. Gardner, ''Qwest Nacchio Sentenced to Six Years, Fined $19 Million,'' *InformationWeek*, July 27, 2007.

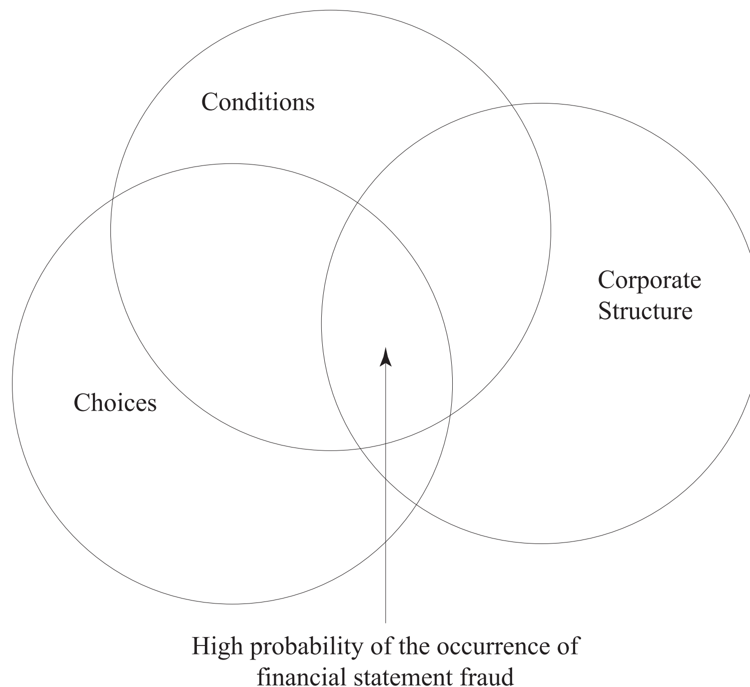


Exhibit 4.1 Interactions of 3Cs of Financial Statement Fraud

Alphonse "Scarface" "Fat Boy" Capone

When no other crimes could be pinned to Al Capone, the Internal Revenue Service obtained a conviction for tax evasion. As the astonished Capone left the courthouse, he said, "This is preposterous. You can't tax illegal income!" But the fact is that income derived from whatever source (legal or illegal) is taxable income. Had money-laundering statutes been on the books in the 1930s, Capone would also have been charged with money laundering.

As noted by John Madinger, in 1930, Alphonse Capone Second Hand Furniture, Inc. grossed more than $105 million in revenue, a staggeringly large number for the times, and paid $32.5 million in cash dividends. The organization's "subsidiaries" included the "beverage division," "gaming division," "entertainment division," and "insurance and industrial relations," as well as corporate governance: officers and directors. Capone's group also engaged in mergers and acquisitions, sometimes by hostile takeover. According to Mardinger, what set Capone apart from other gangsters was that a full third of his revenues was spent on lobbying activities: kickbacks to politicians and law enforcement officials that amounted to a wholesale corruption of the political and government processes in Cook County, Illinois. The Capone organization also kept very good records, tracking receipts and expenditures because no one in the organization wanted to lose an argument over money, a loss that might be terminated with a baseball bat.

Capone was sentenced to 11 years of hard time, serving some of his sentence on the "The Rock" (Alcatraz). With time off for good conduct, he was released in 1939. He lived another eight years in Miami, Florida, where he died at age 48 of heart failure.

Sources: John Madinger, *Money Laundering: A Guide for Criminal Investigations* (Boca Raton, FL: CRC Taylor and Francis, 2006). IRS, "Overview—Money Laundering"; available at www.irs.gov. Associated Press, "Capone Dead at 48; Dry Era Gang Chief," January 26, 1947.

FINANCIAL STATEMENT FRAUD PREVENTION

Exhibit 4.2 presents prevention, detection, and correction mechanisms to reduce the likelihood of financial statement fraud. This continuous mechanism is the most effective way to prevent financial statement fraud. Some elements of this continuous mechanism are:

- Effective corporate governance
- A corporate code of conduct
- Vigilant board of directors including the audit committee
- An adequate and effective internal control structure
- An internal audit function
- External audit services

Corporate governance is responsible for establishing and monitoring ongoing mechanisms that identify and eliminate the causes of financial statement fraud by

Exhibit 4.2 Financial Statement Fraud: Prevention and Detection

Prevention

1. Vigilant board of directors
2. Vigilant audit committee
3. Diligent management
4. Adequate and effective internal audit function

Detection

1. Adequate and effective internal control structure
2. Responsible legal counsel
3. Alert, skeptical external audit assurance function
4. External regulatory oversight procedure

Correction

1. Restatement of current-year fraudulent financial statements
2. Restatement of current-year and prior-years' fraudulent financial statements
3. Ramification of motives and opportunities contributed to the commission of financial statement fraud
4. Establishment and implementation of strategies to regain public confidence in the integrity, quality, and reliability of financial reports

mitigating the effects of motive, opportunity, rationalization, and lack of integrity. Corporate governance is determined by organizational structure, which defines the decisions made by those in authority, and established decision-making policies and standard operating procedures that conform to the acceptable patterns of behavior.

Behaviors that are consistent with the defined set of norms and expectations are perceived to be legitimate. When these cognitive frameworks of corporate governance become firmly established, they begin to define the corporate culture, or the way things are done. Corporate governance that is consistent with the structures and decision-making routines as well as patterns of behavior of one company may be different and inconsistent with the structures of another company. Companies that choose to act illegally select a behavior that many other companies would not consider to be normal or within their set of socially acceptable behaviors. Thus, companies that choose to engage in fraudulent financial activities choose an accounting alternative from a set of both generally accepted accounting methods and unaccepted, primarily illegal accounting methods to prepare their financial statements.

Lack of responsible corporate governance does not necessarily mean that the company will engage in financial statement fraud. There must be both a reason for the company to act illegally and an opportunity for it to engage in the preparation

and dissemination of fraudulent financial statements. A company may engage in issuing fraudulent financial statements if it finds a set of acceptable accounting alternatives to justify its actions; it seizes the opportunity to commit illegal action. The commission of financial statement fraud can be made possible when the 3Cs—conditions, corporate structure, and choices—are present. Thus, the most effective mechanism for preventing financial statement fraud is to focus on the 3Cs and assess their effects on financial statement fraud.

FINANCIAL STATEMENT FRAUD DETECTION

Prevention of financial statement fraud is the best strategy to ensure the quality and integrity of financial reports. However, companies often cannot prevent occurrences of financial statement fraud. Thus, internal and/or external auditors should detect any financial statement fraud that could not be prevented as quickly as possible. Financial statement fraud can be detected by identifying signals associated with fraud, so-called red flags. Several reports have provided lists of red flags indicating early-warning signals of potential financial statement fraud. Chapter 5 thoroughly examines use of the red flag approach to detect financial statement fraud. Observation of an individual's lifestyle and habits in addition to related changes may provide some indication of red flags that may indirectly indicate financial statement fraud (e.g., spending more money than the salary justifies, drinking excessively, becoming irritable easily, not relaxing, taking drugs).

Because the focus of this book is on financial statement fraud perpetrated by management in an attempt to mislead users of financial statements, especially investors and creditors, special attention is placed on identifying business red flags. Business red flags are those conditions and circumstances that arise from the perceived need to overcome financial difficulties, such as an inability to meet analysts' forecasts, increased competition, and cash flow shortages. Management often views these financial difficulties as "temporary." It may attempt to overcome such difficulties by manipulating financial statements to make the company look better financially in order to obtain a new loan or issue stock. Examples of conditions and circumstances that should be considered business red flags include:

- Lack of vigilant corporate governance
- Lack of vigilant oversight board and audit committee
- Inadequate and ineffective internal control structure
- Too much emphasis on meeting earnings forecast and expectations
- Domination of business decision by an individual or a small group
- Aggressive managerial attitude in meeting unrealistic corporate goals
- Company profit exceeds the industry average profit
- Existence of material and unusual related party transactions

- Significant turnover in accounting personnel
- Frequent disputes with independent auditors

CORRECTION PROCEDURES

Correction mechanisms for preexisting financial statement fraud are reactive steps taken by companies to eliminate the committed fraud and its impact on the quality, reliability, and integrity of financial statements. These steps are also taken to prevent further occurrence of fraud. Correction mechanisms are designed to:

- Restate the current year's fraudulent financial statements
- Restate the current year as well as prior years' fraudulent financial statements
- Identify the 3Cs (conditions, corporate culture, choice) and assess their impact on further occurrences of financial statement fraud
- Eliminate motives and opportunities that contributed to the financial statement fraud
- Establish and implement strategies to regain public confidence in the integrity, quality, and reliability of the financial reporting process
- Reassess the impact of the committed financial statement fraud on the established fraud prevention and detection strategies, as well as to continuously monitor the effectiveness of the process of implementing these strategies

PREVENTION, DETECTION, AND CORRECTION STRATEGIES

Publicly traded companies should establish fraud prevention, detection, and correction strategies to effectively monitor the 3Cs presented in this chapter. Examples of these strategies include:

- Establishing a responsible corporate governance, vigilant board of directors and audit committee, diligent management, as well as adequate and effective internal audit functions
- Using an alert, skeptical external audit function, responsible legal counsel, adequate and effective internal control structure, and external regulatory procedures
- Implementing appropriate corporate strategies for correction of the committed financial statement fraud, elimination of the probability of its future occurrences, and restatement of confidence in the financial statement process

Interactions of these three strategies of prevention, detection, and correction are depicted in Exhibit 4.3.

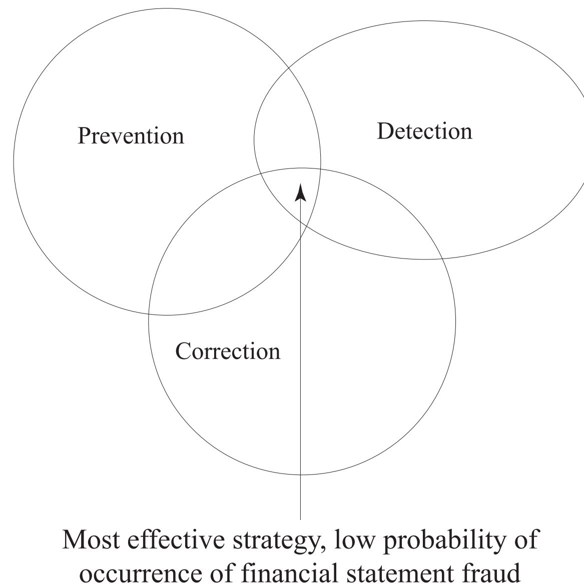


Exhibit 4.3 Interactive Fraud Prevention, Detection, and Corrective Strategies

When these strategies are performed properly and effectively, the opportunity for financial statement fraud is substantially reduced. Financial statement fraud occurs when one or a combination of these strategies is relaxed because of self-interest, lack of due diligence, pressure, overreliance, or lack of dedication. The opportunity for financial statement fraud to occur is significantly increased when these strategies are inadequate and ineffective.

FRAUD AWARENESS EDUCATION

Awareness education can play an important role in reducing instances of financial statement fraud. A 2007 survey conducted by Ernst & Young indicates that the majority of respondents (over 68 percent) do not have any antifraud prevention program and they did not consider their fraud controls to be effective.[6] These results suggest that companies of all sizes should identify and assess fraud risks and design antifraud controls and incorporate antifraud measures into their business operations. Antifraud education and training programs should be provided to employees so they can understand the fraud triangle of incentives/pressures, opportunities, and rationalizations described in the Statement of Auditing Standards No. 99 and the 3Cs. These programs should incorporate lessons learned from reported fraudulent cases. The top 10 lessons from the Enron scandal that should be valuable to standard-setters, investors, executives, and lawyers are:

1. *The need for principles-based accounting rather than rule-based standards*. The use of rules-based accounting standards encourages a check-the-box mentality, which can lead to the financial shenanigans that occurred at Enron.

Enron auditors stated that its financial statements were prepared in conformity with GAAP while financial statements were misleading and fraudulent.

2. *Mark-to-model rather than mark-to-market was a problem at Enron*. At Enron, nonexchanged traded assets and illiquid private deals were treated similarly, with the use of a mark-to-model computer program that estimated future prices and volatility. The appropriate use of the mark-to-market model is necessary for the proper valuation of the trading assets.
3. *Off-balance sheet transactions*. Several special-purpose entities were created to hide liabilities from investors.
4. *Wall Street analysis does not ''do'' complex*. Due to incompetence or conflicts of interest, Wall Street analysts failed to properly analyze and report on Enron's complex financial schemes.
5. *Ineffective rating agency system*. Credit agencies failed to provide early-warning signals to investors about the Enron fiasco and financial distress.
6. *Beware of, and question, unexpected executive resignations*. Wall Street analysts and investors should have recognized the abrupt and sudden resignation of Jeff Skilling as a sign of Enron's financial difficulties and collapse.
7. *The importance of objective whistle-blowers*. Objective and effective whistle-blowing policies and programs that encourage employees to come forward and bring evidence of corporate irregularities to the proper authorities can be very important in preventing and detecting financial statement fraud.
8. *Objectivity and independence of special investigations by corporate boards*. Enron's internal investigation of its board proved to be ineffective and misleading. It did not reveal financial improprieties that could have prevented Enron's collapse.
9. *Character cannot be compartmentalized*. The appropriate tone at the top, promoting ethical behavior throughout the organization and ethical manners of corporate leaders, both rewards and is important in preventing unethical actions and scandals.
10. *Friends do not let (possibly guilty) friends take the stand in criminal trials*. Greed, arrogance, and an incompetent defense strategy were obvious in the Enron trials of Lay and Skilling.

ANTIFRAUD APPLICATIONS FOR PRACTICE

Cynthia Cooper, vice president of internal audit of WorldCom, whistle-blower, and a *Time* magazine ''Persons of the Year,'' said it well:

> People don't wake up and say, ''I think I'll become a criminal today.'' Instead, it's often a slippery slope and we lose our footing one step at a time.[7]

The fraud triangle (see Exhibit 4.4), developed by Donald R. Cressey, suggests that for first-time fraudsters, three attributes must be present for the fraud to occur: pressure/incentive, opportunity, and attitude/rationalization.

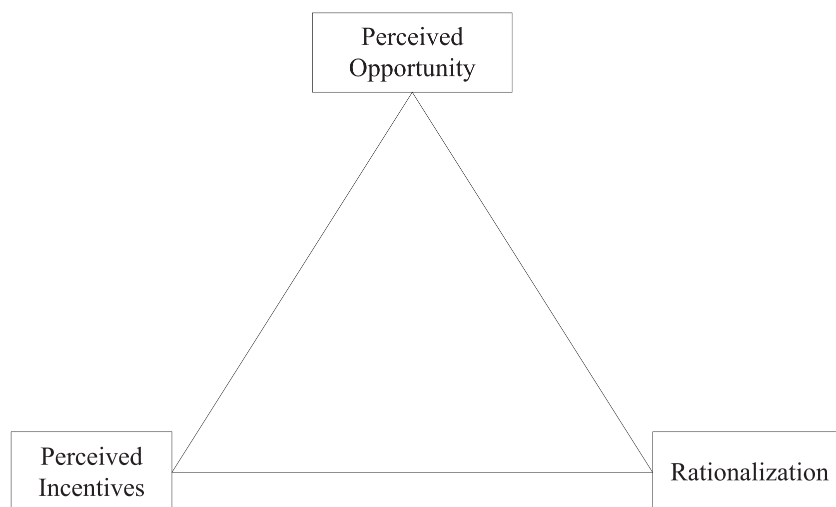


Exhibit 4.4 Fraud Triangle

INCENTIVES/PRESSURE

Pressure is the necessary first step that causes an individual to consider fraud seriously. Fraud pressures often include financial problems: living beyond one's means, greed, high personal debt, poor personal credit, medical bills, investment losses, and children's educational expenses. Financial statement fraud often is associated with less direct pressure, such as meeting analysts' expectations or qualifying for bonuses.

OPPORTUNITY

The second necessary condition is opportunity. Without opportunity, no fraud can exist. Integral ways to reduce opportunity include:

- Establishment of the proper internal control environment
- Adequate training and supervision of personnel
- Effective monitoring of company management by auditors, audit committees, and boards of directors
- Proactive antifraud programs
- A strong ethical culture
- Anonymous hotlines and whistle-blower protections

With regard to financial statement fraud, one of the major challenges is that managers, particularly executive-level managers, can override the system of internal controls. In an organization with ineffective antifraud controls, managers can do just about anything they want. Operationally, this can mean overriding the

control environment to effect financial reporting fraud. Management override can occur in three major ways:

1. The improper use of journal entries
2. The misuse of managerial discretion when it comes to accounting choices, such as important estimates for bad debts, warranties, end-of-period expenses, and so on
3. Misaccounting for unusual, one-time but significant transactions

A related challenge is that financial reporting fraud is often collusive. When a number of people collude, fraud concealment is improved and detection is more difficult.

ATTITUDES OR RATIONALIZATION

Finally, according to Cressey, fraudsters require rationalization or a permissive attitude. Rationalization begs the following question: How do perpetrators sleep at night or look at themselves in the mirror? Rationalizations may include attitudes of:

- "Nobody is getting hurt."
- "It's in the best interest of shareholders and the company."
- "They would understand if they knew the situation."
- "It's for a good purpose."
- "Everyone is doing it."

The following checklists, adapted from the American Institute of Certified Public Accountants' "Management Override of Internal Controls,"[8] provide an overview of pressures, opportunities, and attitudes/rationalizations that can be examined to determine whether the risk of financial statement fraud has increased.

Pressures (Incentives and Motives)

1. Is the entity's financial stability or profitability threatened by global, national economy, or industry conditions?
   - ❒ A high degree of competition?
   - ❒ Market saturation?
   - ❒ Declining industry margins?
   - ❒ An industry vulnerable to rapid change?
     - ❒ Technology

    - ❒ Product obsolescence
    - ❒ Interest rates
  - ❒ Declining industry customer demand?
  - ❒ Anticipated business failures in the industry?

2. Is the entity's financial stability or profitability inconsistent with expectations?
  - ❒ Rapid company growth that runs counter to the industry?
  - ❒ Unusual profitability that runs counter to the industry?
  - ❒ Projected financial results that run counter to industry expectations?

3. Is the entity's financial stability or profitability demonstrating signs of weakness?
  - ❒ Operating losses?
  - ❒ Recurring negative cash flows from operations?
  - ❒ Reported earnings and earnings growth despite negative operating cash flows?
  - ❒ New accounting, statutory, or regulatory requirements?

4. Does excessive pressure exist for management to meet the profitability, incentive goals, budgets, trend expectations, and forward-looking statements contained in the following:
  - ❒ Management press releases?
  - ❒ Annual reports, including Management's Discussion and Analysis of Financial Condition and Results of Operations?
  - ❒ Publicized forecasts or projections?
  - ❒ Communications with:
    - ❒ The board of directors?
    - ❒ Investment analysts?
    - ❒ Institutional investors?
    - ❒ Significant creditors?
    - ❒ Other external parties?

5. Does the entity require additional debt or equity financing, including financing for the following:
  - ❒ Major research and development?
  - ❒ Capital expenditures?
  - ❒ Payroll?
  - ❒ Accounts payable?
  - ❒ Debt repayment obligations?
  - ❒ Debt covenant requirements?

6. Does management perceive adverse effects in reporting poor financial results on significant pending transactions:

- ❐ Credit transactions?
- ❐ New equity investment?
- ❐ Business combinations?
- ❐ Contract awards?

7. Is management's personal financial situation tied to the entity's financial performance (e.g., stock price targets, operating results, financial position, or cash flow):

- ❐ Significant ownership interests in the entity?
- ❐ Compensation:
  - ❐ Bonuses?
  - ❐ Salary increases?
  - ❐ Stock options?
  - ❐ Earn-out arrangements?
- ❐ Personal guarantees of debts within the entity?

8. Are there indications that earnings are expected to be "managed" at the subsidiary or division level:

- ❐ Pressures on lower-level managers to meet expectations?
- ❐ Perception of adverse consequences by lower-level managers if subsidiaries or divisions fail to exceed or fall short of budgeted, projected, or forecasted results?

Opportunities

1. Does the nature of the industry or the entity's operations provide opportunities to engage in fraudulent financial reporting:

- ❐ Related party transactions?
- ❐ Ability to dictate terms or conditions to suppliers or customers?
- ❐ Significant estimates that involve subjective judgments or uncertainties?
- ❐ Significant, unusual, or highly complex transactions, especially near year-end?
- ❐ Operations located or conducted across international jurisdictions?
- ❐ Bank accounts, operations, or related parties located in tax-haven jurisdictions?
- ❐ Significant accounting system changes?
- ❐ Major structural changes (mergers, acquisitions, or spin-offs)?

2. Are there indications that significant estimates used in the annual or quarterly financial reporting process are:
   - ❒ Unrealistic?
   - ❒ Inconsistent with actual historical results?
   - ❒ Inconsistent with the performance of other entities in the same industry?
   - ❒ Inconsistent with past communications with the board of directors (audit committee)?
3. Is there evidence of management's ability to override internal controls:
   - ❒ Domination of decisions by a single person or small group?
   - ❒ Lack of oversight over the financial reporting process and internal controls?
   - ❒ High turnover of senior management, managers, legal counsel, or board (audit committee) members?
4. Is there a complex or unstable organizational structure:
   - ❒ Difficulty in determining ownership interest in the entity and related parties?
   - ❒ Overly complex organizational structure?
   - ❒ Unusual legal entities?
   - ❒ Unusual lines of authority?
5. Are there internal control deficiencies:
   - ❒ Inadequate monitoring of internal controls?
   - ❒ Inadequate fraud risk assessments?
   - ❒ Failure to identify business risks?
   - ❒ Failure to adequately monitor identified risks?
   - ❒ High turnover rates of accounting, internal audit, or information technology staff?
   - ❒ Ineffective or incompetent accounting, internal audit, or information technology staff?
   - ❒ Ineffective or incompetent nonaccounting personnel?

Attitudes and Rationalizations

1. Is there evidence of ineffective or lack of appropriate tone at the top:
   - ❒ Ineffective communication and support of the entity's values and ethical standards?
   - ❒ Communication of inappropriate values or ethical standards?
   - ❒ An unwillingness to address adverse financial statement adjustments or disclosures?

- ❐ A less-than-diligent attitude regarding the entity's antifraud programs and controls?

2. Is there any evidence of excessive preoccupation with:

- ❐ The selection of accounting principles?
- ❐ The determination of significant estimates?
- ❐ Maintaining or increasing the entity's stock price?
- ❐ Maintaining or increasing earnings growth?
- ❐ Committing to analysts, creditors, and other third parties?
- ❐ Minimizing reported earnings solely for tax-motivated reasons?

3. Is there a history of company, related party, or the management team violations of:

- ❐ Securities laws?
- ❐ Other laws?
- ❐ Regulations?

4. Are there pending claims against the entity, related parties, or management:

- ❐ Alleging fraud?
- ❐ Alleging violations of laws and regulations?

5. Has management failed to correct known internal control deficiencies?

6. Have there been repeated or inappropriate attempts by management to justify marginal or inappropriate accounting on the basis of materiality?

7. Is the relationship between management and the current or predecessor auditor strained, as exhibited by:

- ❐ Frequent disputes with the current or predecessor auditor?
  - ❐ Unreasonable demands on the auditor?
  - ❐ Time constraints regarding the completion of the audit?
- ❐ Time constraints on the issuance of the auditor's report?
- ❐ Constraints on the availability of audit evidence?
  - ❐ Restrictions on the auditor's access to people or information?
- ❐ Restrictions on auditor communication with the board of directors or audit committee?
  - ❐ Domineering management behavior?
  - ❐ Attempts to influence the scope of the auditor's work?
- ❐ Attempts to influence the selection or continuance of audit personnel?

The last thought:

Open eyes and a questioning mind are necessary first steps toward fraud prevention and early detection.

NOTES

1. Zachary A. Goldfarb, ‘‘The SEC Charges Stanford Financial in $8B Fraud,’’ *Washington Post*, February 17, 2009.
2. ACFE, ‘‘2008 Report to the Nation on Occupational Fraud and Abuse’’; available at www.acfe.com/documents/2008-rttn.pdf.
3. B. P. Green and T. G. Calderon, ‘‘Information Privity and the Internal Auditor’s Assessment of Fraud Risk Factors,’’ *Internal Auditing* (Spring: 4–15, 1996).
4. State Board of Administration of Florida, ‘‘Corporate Governance Annual Report 2006’’; available at www.sbafla.com/fsb/Portals/6/CorpGovernance/Mutual%20Funds%20Governance%20(2007).pdf.
5. Qwest: www.qwest.com/about.
6. Ernst & Young, ‘‘From Compliance to Competitive Edge: New Thinking on Internal Control,’’ April 2007; available at www.ey.com.
7. Cynthia Cooper, *Extraordinary Circumstances: The Journey of a Corporate Whistleblower* (Hoboken, NJ: John Wiley & Sons, 2008).
8. AICPA, ‘‘Management Override of Internal Controls: The Achilles’ Heel of Fraud Prevention,’’ 2005; available at www.aicpa.org/audcommctr/download/achilles_heel.pdf.

Chapter 5

Taxonomy and Schemes

INTRODUCTION

From at least the first quarter of 2000 through the fourth quarter of 2001, the Security and Exchange Commission (SEC) alleged that Bristol-Myers Squibb engaged in a fraudulent scheme to deceive the investing public about its revenue performance, profitability, and growth trends. Further, to support and conceal the scheme, Bristol-Myers Squibb offered false and misleading representations concerning the Company's performance and profitability. The schemes by which Bristol-Myers Squibb inflated its results included channel stuffing, improper revenue recognitions, using ''cookie jar'' reserves to further inflate its earnings, and failing to accrue properly for Medicaid and prime vendor rebate liabilities.[1]

Management may engage in financial statement fraud to make the company look good financially. Auditors should have a healthy skepticism when auditing financial statements. Antifraud programs and procedures should be developed to identify fraud schemes and to deter, prevent, and detect (as early as possible) their occurrences. Effective antifraud programs should address corporate culture, control structure, and fraud procedures. This chapter presents financial symptoms, including illegitimate earnings management techniques, employed to commit financial statement fraud. Taxonomies of financial statement fraud are developed to identify common fraud schemes and related red flags. The effectiveness of the red flag approach and a model of the whistle-blowing process that can be used in detecting financial statement fraud are also examined in this chapter.

SYMPTOMS OF FINANCIAL STATEMENT FRAUD

Financial statement fraud can be classified into the general categories of accounting schemes and evidence schemes.[2] Accounting schemes are those fraudulent methods through which management perpetrates fraud by manipulating account balances or by disclosing financial items. Evidence schemes are those actions performed by managers to create or hide evidence to conceal fraud. KPMG presents this classification of fraud:[3]

- Fraudulent financial reporting, such as improper revenue recognition, overstatement of assets, and understatement of liabilities

- Misappropriation of assets, including theft, embezzlement, payroll fraud, counterfeiting, royalty fraud, and procurement fraud
- Revenue or assets gained by fraudulent or illegal acts, such as deceptive sales practices, accelerated revenue, bogus revenue, and overbilling customers
- Expense or liabilities incurred from fraudulent or illegal acts, such as kickbacks and bribery
- Other misconduct, such as conflict of interest, insider trading, discrimination, environmental violations, antitrust practices, and theft of competitor's trade secrets

Common examples of symptoms that indicate that a company may engage in financial statement fraud are presented next:

- *Continuous deterioration of quality and quantity of earnings.* One of the most significant contributing factors that increases the likelihood of financial statement fraud is a downward trend in both quantity and quality of earnings. Publicly traded companies are required to disclose earnings for the previous three years in their income statement. Thus, both the quality of the reported past three years' earnings, such as the nature of earnings transactions (e.g., nonrecurring transactions, long-term contracts, bill-and-hold transactions), and the quantity of earnings should be investigated in order to determine the likelihood of financial statement fraud.
- *Inadequacy of cash flow.* Management may use several earnings management techniques to boost earnings when cash flows do not adequately support the appearance of increased earnings. Auditors should realize that cash is king and use the cash flow statement to verify the quantity, quality, reliability, and legitimacy of the reported earnings. The financial statement fraud likely exists when there is no balance between reported earnings and cash flows. For example, earnings are moving up while cash flows are drifting downward.
- *Overstatement of inventories.* Overstatement of inventories and receivables may indicate symptoms of financial difficulties and the possibility of financial statement fraud. Inventory and accounts receivable frauds are commonly used schemes by management to manage earnings and improve the company's financial position. Inventory fraud is one of the most common contributing factors to financial statement fraud because the accounting is complex and the valuation is challenging. To effectively prevent and detect inventory fraud, the inventory observation audit team should include experienced, competent, and skeptical personnel who pay special attention to inventories that appear not to have been used for some time or that are stored in unusual locations or manners. Senior auditors are also required to consider inventory valuation carefully.
- *Overly aggressive accounting.* Another important contributing factor to financial statement fraud is the company's use of aggressive accounting principles,

methods, and practices in areas such as revenue recognition, depreciation and amortization, and capitalization and deferral of costs. The use of such accounting practices provides a warning that management may engage in financial statement fraud in an attempt to improve the appearance of operational results, financial position, and cash flows.

- *Management ''short-termism.''* The issue of whether quarterly reporting, particularly earnings guidance, encourages short-termism and thus compromises financial reporting quality or improves market efficiency has recently been debated within the business community and among policy makers, regulators, and standard setters. Proponents argue that the presentation of quarterly earnings guidance improves market efficiency by reducing analysts' forecast errors and dispersions.[4] Indeed, regulators, including the SEC, continue to promote quarterly reporting by reducing the deadlines for registrants from 45 days to 35 days. Opponents view quarterly earnings guidance as damaging to sustainable financial performance and reporting by encouraging short-termism.[5] Arguments against the detrimental effects of discounting earnings guidance are mounting and center around one key issue. While ending earnings guidance may have a short-term impact on market efficiency and thus require interim trading updates, in the long term it will lead to substantial reduced pressures on management from the market to meet short-term targets.

Bristol-Myers Squibb: Stuffing the Channels

In February 2002, Bristol-Myers Squibb initiated an internal investigation of wholesaler incentives. On April 3, 2002, the company announced that its past earnings projections were ''dramatically off track'' and warned investors that its 2002 earnings could drop by as much as 46 percent, in part because of anticipated wholesaler destocking in 2002. By October, Bristol-Myers Squibb announced that it expected to restate approximately $2 billion in sales primarily from fiscal years 2000 and 2001 due to revenue recognition timing errors.

The schemes by which Bristol-Myers Squibb inflated its results included:

- Channel stuffing, which included stuffing its distribution channels with large quantities of its pharmaceutical products ahead of demand, creating excess inventory at its wholesale customers. The scheme was perpetrated to meet sales and earnings projections set by the company's officers.
- Other improper revenue recognition. It recognized upon shipment approximately $1.5 billion in revenue from consignment-like sales associated with the channel stuffing.
- Using ''cookie jar'' reserves to further inflate its earnings.
- Failing to accrue properly for Medicaid and prime vendor rebate liabilities.

One of the underlying pressures for the channel stuffing and other activities were growth commitments known as double-double and mega-double. In 1994, Bristol-Myers Squibb announced its double-double goal: to double Bristol-Myers Squibb's sales, earnings, and

(*continued*)

earnings per share in a seven-year period. The double-double required average compound annual growth of approximately 10 percent. The last year of the double-double was 2000, and at the end of the year, Bristol-Myers Squibb announced that it had achieved its goal, having "virtually" doubled its sales since 1993. Then, in September 2000, Bristol-Myers Squibb announced mega-double, a plan to double year-end 2000 sales and earnings by the end of 2005, a five-year period. Achievement of the mega-double required average compound annual growth of nearly 15 percent.

Some of the sales incentives that Bristol-Myers Squibb used to induce wholesalers to take excess inventory each quarter included extended payment terms. In at least one case, Bristol-Myers Squibb guaranteed a wholesaler an annualized return on investment of at least 25 percent on any excess inventory. The cost of these guarantees was returned to the wholesaler primarily in the form of price discounts on future sales. Not surprisingly, the sales incentives were costing the company millions of dollars each quarter, and such costs were increasing over time.

The company never admitted guilt. However, Frederick Schiff, Bristol-Myers's former senior vice president and chief financial officer, as well as Richard Lane, former executive vice president of the company's worldwide medicines group, were charged with conspiracy and securities fraud. The SEC followed up the criminal indictments with civil fraud charges.

Sources: U.S. Securities and Exchange Commission v. Bristol-Myers Squibb, U.S. District Court of New Jersey, August 4, 2004. Department of Justice, "Deferred Prosecution Agreement–Bristol-Myers Squibb" (June 13 and 15, 2005). Jeffrey Gold, "Bristol Myers Reaches $300 Million Settlement," Yahoo! Finance, June 16, 2005. Dean Starkman, "Civil Charges Follow Indictments in Bristol-Myers Case," *Washington Post*, August 23, 2005.

IMPROPER REVENUE RECOGNITION

The COSO report[6] indicates that 50 percent of the studied companies that committed fraud overstated revenues by recording revenues prematurely or by creating fictitious revenue transactions. Some examples of schemes used to engage in such fraudulent financial activities include:

- Sham sales
- Premature revenues before all the terms of the sale were completed
- Conditional sales
- Improper cutoff of sales
- Improper use of the percentage of completion method
- Unauthorized shipments
- Consignment sales

These fraud schemes are thoroughly examined in the next section.

OVERSTATEMENT OF ASSETS

The COSO report reveals that about 50 percent of the studied fraud companies overstated assets by recording fictitious assets or assets not owned, capitalized items that should have been expensed, inflated existing asset values through the use of higher market values, and understated receivable allowances.

Asset accounts most commonly misstated, in the order of ranking of frequency, are:

- Inventory
- Accounts receivable
- Property, plant, and equipment
- Loans/notes receivable
- Cash
- Investments
- Patents
- Oil, gas, and mineral reserves

OTHER FRAUD SCHEMES

Other fraud schemes identified in the COSO report include:

- Understatement of expenses and liabilities (only 18 percent of financial statement fraud)
- Misappropriation of assets (only 12 percent of the studied 204 fraud cases)
- Improper disclosures with no financial statement line item effects (about 8 percent of fraud cases)
- Other miscellaneous fraud schemes (20 percent of identified financial statement fraud cases)

COMMON FRAUD SCHEMES

Financial statement fraud consists of a wide variety of schemes, ranging from overstatements of revenues and assets to omission of material financial information to understatement of expenses and liabilities. Exhibit 5.1 presents some of the most common financial statement fraud schemes. Examples are:

- *Misclassification of gains.* This method often is involved in classifying extraordinary or nonoperating gains as part of the income from continuing operations.
- *Sham transactions.* Such transactions typically are associated with coconspirators for whom the scheme is intended to benefit.

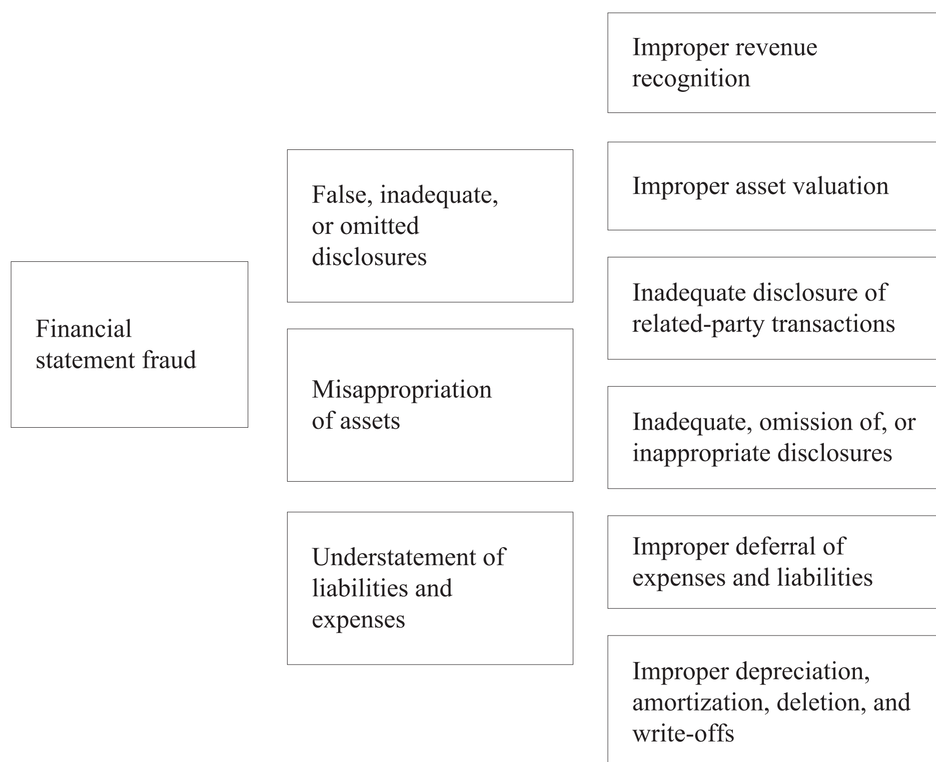


Exhibit 5.1 Most Frequently Used Fraud Schemes

- *Timing of revenue recognition.* Timing usually consists of early recognition of income intended to overstate sales, which are typically fictitious. Many revenue frauds involve improper cutoffs as of the end of the reporting period.
- *Bill-and-hold sales transactions.* Such transactions take place when the customer agrees to buy goods by signing the contract but the seller retains possession until the customer requests shipment. Companies can manage earnings by the early recognition of bill-and-hold sales transactions.
- *Side arrangements.* Such arrangements often involve sales with conditions set by the purchaser, such as acceptance, installation, and adaptability. Side agreements typically alter the terms of a written sale agreement or purchase order by including unilateral cancellation, termination, or other privileges for the customer to avoid the transaction. Side agreements can result in overstatement of revenue, which is an important contributing factor to the occurrence of financial statement fraud. Side agreements often are discovered by transaction confirmations with the outside party, where the vendor or customer is asked to confirm the contract terms and confirm that the contract contains all of the terms and conditions that exist.
- *Illegitimate sales transactions.* Such transactions typically are related to recording fictitious sales involving either phantom customers or real customers

with false invoices, which are recorded in one reporting period (overstatement) and reversed in the next reporting period.

- *Improper revenue recognition.* This consists of inappropriate use of percentage of completion method of accounting for long-term contracts. Management deliberately misrepresents the percentage of project completion when the project is less complete than the amount reflected on the financial statements and often corroborated by fabricated documents.
- *Improper related-party transactions.* These transactions result from the company engaging in less than arm's-length transactions with its top executives or affiliated companies.
- *Improper asset valuations.* Improper valuations often are involved in business combinations of recording fictitious inventory, accounts receivable, or fixed assets as well as improper valuations of these assets.
- *Improper deferral of costs and expenses.* Improper deferral often involves failure to disclose warranty costs and expenses, inappropriate capitalization of expenses, and omissions of liabilities.
- *Inadequate disclosure or omission of material financial information.* These transactions often are associated with deliberate actions by management not to disclose material financial information in the financial statements, in related footnotes, or in management's discussion and analysis.
- *Improper cutoff of transactions at end of reporting period.* This often is associated with interim quarterly financial statements, which are typically carried on into annual financial statements.

COMMON REVENUE FRAUD SCHEMES

Former SEC chair Arthur Levitt describes illegitimate earnings management practices of improperly boosting reported earnings by manipulating the recognition of revenue as "hocus-pocus accounting."[7] The most common methods of illegitimate earnings management are the bill-and-hold transaction and a wide variety of sham transactions involving shipping, billing, and/or related-party transactions.

BILL-AND-HOLD SCHEMES

Corporations often use bill-and-hold schemes to overstate earnings in an attempt to meet or exceed analysts' expectations, especially for quarterly earnings forecasts. In a bill-and-hold deal, the customer agrees to buy goods by signing the contract, but the seller retains possession until the customer requests shipment. The seller may recognize revenue in compliance with existing GAAP because the transaction meets the two conditions of (1) realized or realizable and (2) earned, as required by

GAAP. Revenues usually are recognized at the time of sale, which is often when delivery of goods occurs or services are rendered to customers. While bill-and-hold sales transactions are not necessarily a GAAP violation, corporations often use such transactions to manage earnings illegitimately, which may result in financial statement fraud. Thus, auditors should assess the substance of such transactions to make sure they are legitimate and arm's-length transactions.

The SEC has specified in its enforcement actions that transactions that meet the next criteria can be recognized as revenues:

- The company must have a fixed commitment to purchase from the customer, preferably in writing.
- The risks of ownership must have passed to the buyer.
- The buyer, not the seller, must have requested the transaction and must have a legitimate business purpose of a bill-and-hold deal.
- The seller must not retain any significant specific performance obligations, such as an obligation to assist in resale.
- There must be a fixed delivery date that is reasonable and consistent with the buyer's business purpose.
- The goods must be complete and ready for shipment and not subject to being used to bill other orders.[8]

SHAM TRANSACTIONS

Sham transactions typically are associated with financial statement fraud. They appear to be legitimate sales, but they are not. Examples of sham transactions include:

- Sales with a commitment from the seller to repurchase
- Sales without substance, such as funding the buyer to assure collection
- Sales with a guarantee by an entity financed by the seller of what would otherwise be considered as an uncollectable receivable
- Sales for goods merely shipped to another company location (e.g., warehouse)
- Premature revenues before all the terms of the sales were completed by recording sales after the goods were ordered but before they were shipped to the customers or shipping in advance of the scheduled date without the customer's knowledge and instruction

IMPROPER CUTOFF OF SALES

Improper cutoff of sales involves keeping the accounting records open beyond the reporting period to record sales of the subsequent reporting period in the current

period. This scheme is more effective to manipulate quarterly revenue than annual revenue by keeping books open so revenue is recorded in that quarter.

CONDITIONAL SALES

Conditional sales are transactions recorded as revenues even though the sales associated with transactions involve substantial unresolved contingencies or subsequent agreements that eliminate the customer's obligations to retain the merchandise.

David Jacob Levi Chen (a.k.a. Crazy Eddie): A Financial and Legal Odyssey

Eddie Antar, who disappeared in 1989 after the demise of his Crazy Eddie consumer electronics chain, was arrested in June 1992 near Tel Aviv. Antar, 44 years old at the time of his arrest, was discovered by the Israeli police to be living in a luxurious town house in Yavne, a town in central Israel, under the name David Jacob Levi Cohen.

In 1996, Crazy Eddie pleaded guilty to a federal charge that he had defrauded shareholders of more than $74 million by manipulating the company's stock. His plea agreement ended a seven-year financial and legal odyssey, including Antar's disappearance and flight under an assumed name to Israel to avoid arrest.

In the 1980s, Antar and several family members built Crazy Eddie into the largest consumer electronics chain in the New York area. Commercials, in which a fast-talking announcer boasted that the stores' prices were "insaaane," became standard television fare. The company went public in 1984. By falsifying its books, Antar convinced financial analysts that Crazy Eddie was growing when, in fact, it was falling apart. When auditors were on the verge of discovering the scheme, company executives took the falsified documents and threw them in the garbage, according to testimony by the company's chief financial officer, Sam Antar.

In 1992, Eddie Antar was convicted by a federal jury in Newark on 17 separate charges, including conspiracy, racketeering, and securities fraud. Those convictions, however, were overturned by the United States Court of Appeals. Similarly, his brother, Mitchell Antar, had his convictions in the Crazy Eddie case thrown out. Ultimately, both Antars ended up with jail sentences: Eddie with 6 years 10 months and Mitchell with 1.5 years.

Sources: Adam Bryant, "Crazy Eddie's Chief Is Arrested in Israel," *New York Times*, June 25, 1992. Barry Meier, "Founder of Crazy Eddie Chain Pleads Guilty in Stock Fraud," *New York Times*, May 9, 1996. Lisa W. Foderaro, "Crazy Eddie's Returning, Minus 2 Jailed Founders," *New York Times*, January 20, 1998. Associated Press, "Crazy Eddie Profits Sought," *New York Times*, July 16, 1998.

FINANCIAL STATEMENT FRAUD RED FLAGS

Different types of fraud have different symptoms (or better known as red flags) with respect to financial statement fraud. Red flags are important symptoms, which signal the likelihood of financial statement fraud. Both internal and external

auditors are well qualified and positioned to identify the red flags and develop a risk model to prevent and detect financial statement fraud. However, internal auditors' involvement in the routine activities of the corporation and internal control environment place them in the best position to identify and assess evidence that may signal financial statement fraud.

Qualitative red flags are important pieces of evidence for signaling the likelihood of financial statement fraud. A proper focus on red flags can assist in exploring the underlying factors that cause financial statement fraud. Possible symptoms of financial statement fraud are compiled from several studies and reports, and they are listed in three general categories of (1) organizational structure, (2) financial conditions, and (3) business and industry environments. SAS No. 99 defines red flags in terms of risk factors in the three categories included in the fraud triangle: pressures/incentive, opportunity, and attitudes/rationalizations. Albrecht and Albrecht[9] identify six symptoms of fraud:

1. Accounting anomalies
2. Internal control weaknesses
3. Analytical anomalies
4. Extravagant lifestyles
5. Unusual behaviors
6. Tips and complaints

According to Elliot and Willingham,[10] red flags do not indicate the presence of fraud. Rather, they are conditions that commonly are present in events of fraud and thus they suggest that concern may be warranted. Exhibit 5.2 presents a list of red flags.

CHANNELS FOR COMMUNICATING WRONGDOING

Ponemon[11] and Hooks et al.[12] describe internal and external channels for communicating sensitive issues such as financial statement fraud. The internal channel refers to disclosing wrongdoing to coworkers, top management, the audit committee, and/or the board of directors. External channels can be used to communicate wrongdoing to those outside of the company, such as media, external auditors, and/or a governmental agency. Whistle-blowers typically use internal channels as their first and often only course of action for communicating sensitive issues such as financial statement fraud, primarily because external disclosure may be viewed as a violation of business etiquette, employee loyalty, corporate code of conduct, and/or professional standards. For example, internal auditors are required to refrain from disclosing wrongdoing to individuals outside of their organizations in accordance with the Institute of Internal Auditors Statement of Internal Auditors Standards No. 3.[13] Nevertheless, external challenges should be employed as a last

Exhibit 5.2 Red Flags

Organizational Structure Red Flags Culture

- Inappropriate "tone at the top"
- Nonexistent corporate code of conduct
- Overly complex organizational structures
- Frequent organizational changes
- Irresponsible corporate governance
- Decentralized organization structure without adequate monitoring
- Morale is low, especially among top executives and managerial employees
- High turnover within the company, especially at top executive level
- Maximizing profits is the corporate mission

Board Characteristics

- Predominantly insider or "gray" board of directors
- Ineffective board of directors
- Lack of vigilant board of directors' oversight
- Lack of or ineffective mechanisms for reporting management violations of company policy
- High percentage of inside and financially interested members on the board of directors
- Failure to require top executives to take at least a week's vacation at a time
- Failure to pay attention to details
- No proper enterprise risk management
- Too much trust in key executives

Audit Committee Characteristics

- Ineffective, financially illiterate, and incompetent audit committee
- Nonexistent or ineffective audit committee
- Inadequate response to the risk of collusion and management override
- Lack of adequate and effective internal control structure
- Ineffective internal control over financial reporting
- No or ineffective communication between the audit committee and external auditors
- No or infrequent meetings between the audit committee and internal auditors
- Management reluctant to cooperate with external auditors or consider external auditors' suggestions and recommendations
- Frequent disputes between management and external auditors
- Management engaged in opinion shopping
- Management is overly evasive when responding to audit inquiries

(*continued*)

Exhibit 5.2 (continued)

- Untimely reporting and responses to audit committee inquiries
- Providing information to auditors at the last minute

Internal Audit Characteristics

- Nonexistent or ineffective internal audit function

Auditor Characteristics

- Frequent changes of external auditors
- Lack of cooperation and coordination between internal and external auditors
- Management placing undue pressure on auditors

Managerial Characteristics

- A highly domineering top management team
- Compensation for top executives tied to earnings or stock price targets
- Frequent turnover of senior management
- Inexperienced management team
- Autocratic management
- Excessive or inappropriate performance-based compensation
- Rapid turnover of key personnel (either quit or fired)
- Ineffective leadership
- Lack of personnel evaluation
- Inexperienced and aggressive personnel in key positions
- Use of several legal counsels
- Use of several different banks for specified purposes
- Conflict of interests within company management
- Executives with record of malfeasance
- Significant management compensation derived from performance-based incentive plan
- Company holdings as material portion of management's personal wealth
- Management's job threatened by poor performance
- Management has lied to regulators and auditors or has been evasive
- Management's aggressive attitude toward financial reporting
- Managerial personality anomalies
- Lax attitude toward internal controls and management policy
- Lax attitude toward compliance with applicable laws and regulations
- Poor reputation of management in the business community
- Domination of the company by one or two aggressive individuals
- Key executives with low moral character

- Key executives exhibiting strong greed
- Wheeler-dealer top executives
- Management that attempts to gloss over a ‘‘temporarily’’ bad situation
- Key executives with a strong desire to beat the system
- Management that displays significant disrespect for regulatory bodies
- Management that doesn’t see financial statement fraud as a risk
- Management that ignores irregularities
- Aggressive and egotistical top executives

Economic, Industry, and Environmental Red Flags Economic Characteristics

- High interest rate and currency exposures
- Unfavorable economic conditions

Industry Characteristics

- Business conditions that may create unusual pressures
- Highly competitive global markets
- Industry volatility
- Exposure to rapid technology changes
- Industry softness or downturns
- Unfavorable economic conditions within the industry
- Long business cycle
- Unfavorable merger and acquisition activity
- Product or industry in decline
- Profitability of the company inconsistent with the industry

Regulatory Characteristics

- Ongoing or prior investigation by regulators (e.g., SEC, IRS)
- Suspension or delisting from stock exchange
- Evidence of insider trading
- Uncertain issues relating to public trading of stock
- Significant tax adjustments by the IRS

Financial Performance and Conditions Red Flags Business Conditions

- Unusually rapid growth
- Unusual results or trends
- Overemphasis on one or two products, customers, or transactions
- Excess capacity
- Severe obsolescence

(*continued*)

Exhibit 5.2 (continued)

- High rapid expansion through new business or product lines
- Introduction of significant new products and services
- Significant litigation, especially between shareholders and management
- Continually operating on crisis basis
- Unexpected and sharp decreases in earnings or market share experienced by a company or industry
- Substantial doubt about the company's ability to continue as a going concern
- Highly computerized operations
- Competition from low-priced imports
- Long manufacturing cycle and throughout time
- Adverse legal circumstances
- Unjustifiable and high business risks
- Existence of revocable licenses necessary for continuation of business

Revenue and Earnings Characteristics

- Deterioration of earnings quality as evidenced by a sharp decline in sales volume
- Unrealistic earnings expectations
- Unrealistic growth goals
- Pressure to finance expansion through current earnings rather than through debt or equity
- Progressive deterioration in quality and quantity of earnings
- Unusually high earnings with a cash shortage
- Urgent need for favorable earnings to support high price of stock and meet analysts' earnings forecasts
- Cash shortage or negative cash flows
- Unrealistic budget pressures
- Financial pressure to meet or even exceed analysts' forecasts
- Financial pressure resulting from bonus plans tied to earnings performance
- Earnings deterioration resulting from significant decreases in revenues or substantial increases in expenses
- Aggressive attempts to maintain or reverse trends and achieve forecasts
- Operating results inconsistent with macroeconomic industry
- Aggressively optimistic operating and financial budgets
- Pressure to meet investors' high expectations through budgeting process
- Rapid increase in earnings
- Salary structure, especially for top executives, is tied to profits
- Understated costs and expenses
- Sizable increases in inventory without comparable increases in sales

Transaction Characteristics

- Overly complex and unusual business transactions
- Heavy investment losses
- Long-term financial losses
- Several losses from major investments
- Significant difficult-to-audit transactions
- Unusual and large year-end transactions
- Unsupported or unauthorized journal entries
- Unsupported or questionable discretionary accounting estimates
- Many adjusted entries required as a result of the time of audit
- Use of liberal accounting practices
- Inadequate accounting information system
- Significant related-party transactions
- Material account balances determined by judgment
- Unusual and significant contractual commitments
- Numerous acquisitions of speculative ventures in pursuit of diversification

Balance Sheet Characteristics

- Lack of adequate working capital
- Extremely high debt
- Tight credit, high interest rates, and reduced ability to acquire credit
- Difficulty in collecting receivables
- The need for additional collateral to support existing obligations
- Significant off-balance sheet or contingent liabilities
- Inadequate collectability reserves
- Debt restrictions with little flexibility
- Significant inventories and other assets that require special expertise for valuation
- Little tolerance on debt restrictions

resort for communicating wrongdoing when the internal communication fails to resolve the problem.

External auditors are required to use both internal and external channels in communicating sensitive issues such as financial statement fraud. Section 301 of the Private Securities Litigation Reform Act of 1995, entitled "Fraud Detection and Disclosure," requires that external auditors design audit procedures to provide a reasonable assurance of detecting illegal acts that would have a direct and material effect on financial statements (e.g., financial statement fraud). The Reform Act also requires external auditors to inform the appropriate level of management and ensure that the audit committee (or the board of directors if there is

no audit committee) is informed of financial statement fraud. If, after ensuring that the audit committee or the board is adequately informed, the external auditors determine that financial statement fraud warrants departure from a standard audit report or resignation, then the auditors should report the audit conclusion directly to the board of directors. The board, upon receiving such a report, should notify the SEC of the auditors' report no later than one business day thereafter and provide the auditors with a copy of the notice to the SEC. If the board does not act within one business day after the audit report was given to it, the external auditors should resign, which will cause the company to file a Report Form 8-K regarding the resignation of the auditor, or report to the SEC no later than one business day following the failure to receive any notice from the board of directors.

WHISTLE-BLOWER REGULATIONS

Whistle blowing means that an individual with knowledge of wrongdoing, including financial statement fraud, informs those with the authority to remedy the wrong of the situation. In the case of financial statement fraud, the appropriate remedial agency could be members of management not involved in the fraud, the board of directors, audit committees, internal auditors, external auditors, or outside regulatory or law enforcement bodies such as the SEC. Gamesmanship, however, is when the person with knowledge of wrongdoing, including financial statement fraud, voluntarily or *compulsorily* participates with the wrongdoers to cover up or commit the fraud. The process of a whistle-blowing report starts with an important wrongdoing, such as financial statement fraud. The observer of the act may choose to report to a party empowered to at least begin resolution, such as the observer's superior, internal auditors, the audit committee, or external auditors. Then, after assessing the costs and benefits as well as other considerations (e.g., retaliations, lost of job perceived lack of loyalty), the observer may decide to report.

Time magazine's 2002 Persons of the Year were three courageous women: Sherron Watkins of Enron, Cynthia Cooper of WorldCom, and Coleen Rowley of the FBI, who put everything on the line to do the right thing by standing up to corporate wrongdoers and coming forward to report fraud. Prior to the passage of SOX, there were no required whistle-blower programs or complaint mechanisms for employees to take proper actions to report corporate wrongdoings to authorities or persons in a position to prevent and correct them. SOX requires the company's audit committee to establish whistle-blowing procedures for the receipt, retention, and treatment of public company complaints.[14] The programs must implement procedures and mechanisms that encompass the confidential and anonymous submission of concerns on questionable accounting and auditing matters by employees. Whistle-blowing programs and procedures can also be established in organizations of all types and sizes.

Section 301 of SOX requires audit committees to establish procedures for the receipt, retention, and treatment of complaints from outsiders or insiders regarding accounting, auditing, and internal control issues. Section 806 of SOX prohibits public companies from discharging, demoting, suspending, threatening, harassing, or discriminating against whistle-blowers (e.g., officers, employees, contractors, subcontractors, agents) because of any lawful acts done by whistle-blowers to assist an investigation of violations of securities laws by the company. To comply with the requirements, public companies should establish both internal and external whistle-blower programs. An external whistle-blower program is designed to facilitate the receipt, retention, and treatment of complaints received from parties outside an organization, including customers, suppliers, investors, and creditors. An internal whistle-blower program deals with parties inside an organization (employees). Internal whistle-blower programs enable corporations to take a proper course of action to correct improper activities, particularly those related to accounting, reporting, internal controls, and operational issues, without the adversarial effects of possible public disclosure.

Section 301 of SOX regarding whistle-blower mechanisms for the receipt, retention, and treatment of complaints covers only internal and external accounting, auditing, and internal control matters. SOX does not address general complaints regarding customer or supplier dissatisfaction and employment-related issues. Nevertheless, it is appropriate that the audit committee, in establishing whistle-blower programs to meet the mandatory regulatory requirements, also consider and incorporate general complaints in addition to auditing, accounting, and internal control complaints. The audit committee should oversee the company's whistle-blower programs' procedures and complaint mechanisms, which are designed for concerned individuals to report wrongdoings to authorities or persons in a position to prevent and correct wrongdoings.

In August 2004, the Department of Labor published final rule 29 CFR Part 1980-Procedures for the Handling of Discrimination Complaints Under Section 806 of the Corporate and Criminal Accountability Act of 2002, Title VIII of the Sarbanes-Oxley Act of 2002, establishing Occupational Safety and Health Administration (OSHA) administrative procedures for handling whistle-blower discrimination complaints under Section 806 of the Sarbanes-Oxley Act, which is just one of 14 whistle-blower statutes enforced by OSHA.[15] A corporate employer may not take any discriminatory actions (e.g., discharge, demotion, suspension, threats, harassment, failure to hire or rehire, blacklisting) against or fire an employee who participates in or causes a federal investigation or proceeding. OSHA defines the unfair treatment of any employee with respect to the employee's compensation, terms, conditions, or privileges of employment because the employee, or any person acting pursuant to the employee's request as discriminatory action: Any employee experiencing employer retaliation for corporate whistle-blowing has 90 days after the alleged allegation in which to file a complaint with OSHA. OSHA will begin its agency review of a complaint by determining whether an investigation is necessary. If so, OSHA will conduct an investigation in accordance with the

statutory requirements. OSHA will issue its findings, which can be appealed by either party requesting a full hearing before an administrative law judge of the Department of Labor. If either party is unhappy with the administrative judge's decision, they can seek review of the decision by the department's Administrative Review Board. The employee may file a complaint in the appropriate district court of the United States only if the agency has not issued a final order within 180 days of the filed complaint.

As of 2007, OSHA has completed 1,163 investigation based on employees complaints filed under the provisions of the SOX since its inception.[16] Because public perception of whistle-blowers is now favorable and whistle-blowers now have protection, more employees are coming forward.[17] To avoid regulatory scrutiny and civil action, attorney Jason Zuckerman recommends corporations take these eight steps:[18]

1. Create a policy prohibiting retaliation
2. Train managers and supervisors
3. Establish an employee concerns program
4. Update the employee on the status of the investigation
5. Document the findings in a written report
6. Establish procedures for anonymous reporting
7. Take disciplinary action against those who engage in retaliation
8. Document performance issues

ANTIFRAUD APPLICATIONS FOR PRACTICE

DETECTION: RED FLAGS AND TARGETED RISK ASSESSMENT

Exhibit 5.3 presents the numerous types of revenue and expense fraud schemes that can be perpetrated.[19]

This taxonomy highlights the general types of financial reporting fraud grounded in the income statement. When revenues or expenses are misstated, those must have a corresponding misstatement in the balance sheets as well as in:

- Accounts receivable
- Inventory
- Investments
- Property plant and equipment
- Intangibles and other assets
- Liabilities
- Stockholders' equity
- Related note disclosures

Exhibit 5.3 Financial Statement Fraud Schemes

Fraudulent Revenues and Expenses

Fictitious Customer Revenue

- Invoices to phony companies
- Phony invoices (other documentation) to legitimate customers
- Shipments to customers without an order
- Shipments to noncustomer (e.g., warehouse location)
- Recording accounts receivable collections as revenue
- Recording deposits as revenue
- Recording supplier refunds as revenue
- Round-trip transactions
- Money laundering

Overstated Revenues

- Failing to record markdowns and discounts
- Failing to record sales returns and allowances

Understated Revenues

- Skimming
- Unrecorded sales
- Understated sales
- Delaying sales revenue

Premature Revenue Recognition

- "Channel stuffing"
- Holding the books open to record customer
- Shipments after period end
- "Bill and hold"—recording revenue prior to shipment
- Recording sales that are contingent on a future event
- (e.g., customer financing, consignment goods, right of return, guaranteed return, performance guarantee)
- Recording revenue when future service
- commitments to the customer exist
- Recording revenue when substantial uncertainty
- Exists about the ability to collect the receivable
- Pre-invoicing of work-in-process
- Partial shipments recorded as full shipments
- Overestimating the percentage of completion
- Recording long-term contract revenue based on billings

Expenses

- Capitalizing expenses
- Understated expenses from fraud schemes related to assets and liabilities

Given concerns over management override and collusion, related party (e.g., Enron's special-purpose entities) transactions should be carefully scrutinized. Readers need to understand that every fraudster rationalizes his or her scheme differently. In addition, differing concealment techniques are used, depending on who knows about and is involved in the activity. As such, those assigned with fraud prevention, deterrence, and detection responsibilities may be overwhelmed with the following question: Where to begin?

Traditional approaches suggest that a variety of red flags may indicate that an underlying fraud has occurred or is occurring. A summary of red flags was presented in Exhibit 5.3. The red flags that can lead to a formal fraud investigation include tips

and complaints, behavioral red flags, analytical anomalies, accounting anomalies, as well as internal control irregularities and weaknesses. Each of these, when observed, needs to be evaluated with evidence to make any determination concerning the existence of fraud. Some of the questions that need to be answered are:[20]

- Does the anomaly have supporting documentation?
- Does the supporting documentation appear to be falsified, altered, or fictitious?
- Does the transaction and its reflection in the financial statements make sense?
- Does the transaction make sense in light of the company's operations, goals, and objectives?
- Does the totality of this and similar transactions make sense analytically when evaluated in comparison to the economy, the industry, key competitors, and other related accounting numbers within the organization?
- Does the transaction have proper approval and the proper authority levels?
- Does anything else about the transaction or its nature make it appear suspicious?

Asking follow-up questions and resolving those questions with evidence is one of the keys to professional skepticism and a key to successfully uncovering fraudulent activity, whether asset misappropriation, corruption, or financial statement fraud. The challenge with red flags is that they are numerous and that 1 in 100 may lead to the detection of fraudulent activity.

A refinement to red flag fraud detection, prevention, and deterrence is a targeted risk assessment. In practice, targeted risk assessment has multiple steps but the approach focuses on two major questions:

1. *Given an understanding of the population of fraud schemes that are possible, which schemes are most likely, given this company, its industry, and its operational environment?* For example, the Bristol-Myers Squibb example highlighted channel stuffing. But channel stuffing is most likely when the company sells few products and has a relatively small number of customers, such as wholesalers. Thus, service industries may be susceptible to numerous revenue recognition schemes, but generally channel stuffing is not one of them. By using knowledge of the company, its industry, and its operating environment, the person saddled with fraud risk management can start to focus efforts on those fraud schemes that are most probable.
2. *What is the likely magnitude of the fraud? Alternatively, how significant would the dollars associated with the fraud scheme be in relation to the company's expected financial performance and condition?* By incorporating the magnitude of the fraud scheme into the risk assessment, those involved with fraud risk management can further identify which potential frauds require greater attention. For example, inventory and its related accounting often are associated with a higher likelihood of fraud. However, if the company has minimal inventory because it uses just-in-time inventory management in the manufacturing

processes and inventories are considered immaterial, antifraud efforts with regard to inventory-related frauds may be minimized.

Once these questions have been answered, other questions can be examined:[21]

- How is the fraud scheme rationalized?
- How would I find the fraud?
- Where would the fraud be located in the books and records?
- What attributes are involved in the fraud act?
- Who would have knowledge of fraud scheme?
- Who would be involved: insiders, outsiders, collusive parties, managers overriding the system?
- How would the fraud act be concealed?
- What symptoms (red flags) would be generated if the scheme was perpetrated?
- How is the scheme often detected?
- What controls need to be in place to prevent this particular scheme?
- What controls might deter a fraudster due to increased perception of detection?
- What controls would lead to detection of this scheme?
- Are the controls effective, in place, and functioning properly?
- Which employees, third parties, or managers are likely to be involved, and could it be collusive?

Of course, targeted fraud risk assessment and its related management are more complicated than described, but the suggestions provide a good starting point for evaluating fraud risks within an organization. To be successful, this approach requires professionals not only to understand the company, its competitive environment, and industry but also to understand the various fraud schemes. Management's override of internal controls and collusive behavior often result in fraud schemes with a high degree of probability and significant magnitude. Further, overseas operations are also often considered high risk, due to compliance issues associated with the Foreign Corrupt Practices Act. With regard to these risks, professionals need to pay particular attention.

The last thought:

The trouble with sleight of hand is that you are always looking in the wrong place.

—M. J. Rose, author of *The Reincarnationist*

NOTES

1. SEC, ‘‘$750 Million Distribution Begins for Bristol-Myers Fraud Victims,’’ June 8, 2006.
2. GAO L. and R. P. Strivastava, ‘‘The Anatomy of Management Fraud Schemes: Analyses and Implications,’’ Working paper, 2007.

3. KPMG, ‘‘Cross-Border Investigations, Effectively Meeting the Challenge,’’ 2007; available at www.kpmg.ie/DestinationIndia/pubs/Cross-Border%20Investigations.pdf.
4. P. Healy and K. Palepu, ‘‘Information Asymmetry, Corporate Disclosure and the Capital Markets: A Review of Empirical Disclosure Literature,’’ *Journal of Accounting & Economics* 31 (2001): 405–440.
5. Ernst & Young, ‘‘9th Global Fraud Survey: Fraud Risk in Emerging Markets,’’ 2007; available at www.giaccentre.org/documents/ERNSTYOUNG.FRAUDSURVEY.JUNE06.pdf.
6. COSO, ‘‘Fraudulent Financial Reporting: 1987-1997—An Analysis of U.S. Public Companies (1999).’’ Available at www.coso.org/publications/FFR_1987_1997.PDF.
7. D. R. Carmicheal, ‘‘Hocus-Pocus Accounting,’’ *Journal of Accountancy* (October 1999): 50–55.
8. A. Levitt, ‘‘The Numbers Game,’’ New York University Center for Law and Business (September 1998).
9. W. Steven Albrecht and Chad O. Albrecht (contributing author), ‘‘Fraud Examination,’’ Thomson South-Western, 2003.
10. R. K. Elliot and J. J. Willingham, *Management Fraud: Detection and Deterrence* (New York: Petrocelli Books, 1980), 15.
11. L.A. Ponemon, ‘‘Whistle-Blowing as an Internal Control Mechanism: Individual and Organizational Considerations,’’ *Auditing: A Journal of Practice & Theory* (Fall 1994): 118–130.
12. K. Hooks, S. Kaplan, and J. S. Chultz Jr., ‘‘Enhancing Communication to Assist in Fraud Prevention and Detection,’’ *Auditing: A Journal of Practice & Theory* (Fall 1994): 86–117.
13. Institute of Internal Auditors, *Statements of Internal Auditing Standards No. 3: Deterrence, Detection, Investigation and Reporting of Fraud* (Altamonte Springs, FL: Author, 1985).
14. Sarbanes-Oxley Act, 2002; available at www.soxlaw.com.
15. OSHA, ‘‘OSHA Fact Sheet: Whistleblowers and Corporate Fraud,’’ 2003; available at www.osha.gov/OshDoc/data_General_Facts/whistleblower_rights.pdf.
16. ‘‘OSHA Publishes Final Rule on Whistleblower Procedures under Sarbanes-Oxley Act of 2002,’’ *Professional Safety* 49(10) (October 2004): 16.
17. Jason M Zuckerman, ‘‘Whistle-Blower Protection Programs for Associations,’’ *Association Management* 56(6) (June 2004): 13–15.
18. Ibid.
19. The taxonomy forms the basis of Sarah E. Bonner, Zoe-Vonna Palmrose, and Susan M. Young, "Fraud Type and Auditor Litigation: An Analysis of SEC Accounting and Auditing Enforcement Releases," *Accounting Review* 73, No. 4 (October 1998): 503–532.
20. Joseph Wells, Mary-Jo Kranacher, and Richard Riley, *Fraud and Financial Forensics* (Hoboken NJ: John Wiley & Sons, forthcoming).
21. Ibid.

Part Three

Corporate Governance and Its Role in Preventing and Detecting Financial Statement Fraud

Chapter 6

Role of Corporate Governance

INTRODUCTION

The financial reporting scandals giving rise to the Sarbanes-Oxley (SOX) Act of 2002 generated significant concerns not only because of the size of failures and irregular accounting practices but also because they cast doubt on the ability of corporate governance participants to prevent, deter, and detect material fraud and financial malfeasance. The recent Madoff, Stanford Financial, and Satyam frauds raise serious concerns about systemic regulatory efficacy, ineffective corporate governance, and irresponsible corporate gatekeepers, especially since these frauds broke in late 2008 and early 2009, years after SOX was in place. Three gatekeepers closely associated with corporate governance and the financial reporting process are the board of directors, the independent auditor, and the legal counsel. The question often heard during the reported financial scandals at the turn of the twenty-first century, "Where were the gatekeepers?" is being asked again after the Madoff and Satyam frauds. One obvious example of the gatekeepers' failure to fulfill their professional responsibility is the fraud at Refco Inc., where both the legal counsel and auditors engaged in aiding and abetting fraud, according to the report from an independent examiner appointed by a U.S. bankruptcy court.[1]

Consider Phar-Mor, a company that began in 1982 and had 40 stores by the end of 1987. As it expanded, Phar-Mor increasingly ran into Wal-Mart and began losing money. To allow founder and president Mickey Monus time to fix the operational, pricing, and gross margin issues, Phar-Mor's financial group, headed by Pat Finn, chief financial officer (CFO), began to conceal the company's losses. Ignoring a 1991 memo from Phar-Mor general counsel that described rumors that vendors were refusing to supply inventory because of unpaid bills, David Shapiro, chief executive officer (CEO) and chairman of the board, indicated that the memo should be destroyed. In spring 1992, the scheme unraveled. The Phar-Mor fraud totaled more than $500 million; despite the success it reported in its financial statements, Phar-Mor hadn't earned any income in five years. By the time the smoke cleared, the entire Phar-Mor corporate governance structure claimed to be a victim: the accountants, the auditors, the investors, the chief executive, and the board of directors. All claim it was someone else's responsibility.

Failures like Phar-Mor, Enron, WorldCom, Adelphia, and the 2008 financial meltdown have spurred the demand for ever-improving corporate governance and accountability for business organizations and appear to be a global trend in the post-SOX era. Indeed, the phrase ''corporate governance'' appeared for the first time in any legislative reforms in Section 111 of the Emergency Economic Stabilization Act of 2008[2], better known as the government bailout of troubled financial institutions. The act requires the establishment of executive compensation and corporate governance standards for those financial institutions receiving federal bailout funds. This chapter presents the role of corporate governance in preventing, detecting, and correcting financial statement fraud.

DEFINITION OF CORPORATE GOVERNANCE

The concept of corporate governance is poorly defined in the business literature through both narrow and broad definitions that reflect special interests of different groups in corporate governance. Narrowly defined, corporate governance focuses primarily on the interactions among corporate managers, directors, and shareholders in order to reduce the potential agency problem of aligning interests of management with those of shareholders. This definition of corporate governance addresses the concerns of capital providers in assessing the risk associated with their investment, their expectations for rate of return on investment, and continuous monitoring of their capital investments.

Broadly defined, corporate governance focuses on the combination of applicable laws, regulations, and listing rules that facilitate, direct, and monitor corporations' affairs in attracting capital, performing effectively and efficiently, increasing shareholder value, and meeting both legal requirements and general societal expectations.

Thus, corporate governance is viewed as a mechanism of monitoring the actions, policies, and decisions of corporations in increasing shareholder value.

For the purpose of this book, *corporate governance* is defined as a process of managing, directing, and monitoring a corporation's business to create shareholder value while protecting interests of other stakeholders (creditors, suppliers, government, and society). A similar definition of corporate governance is adopted by Rezaee in *Corporate Governance Post Sarbanes–Oxley*.[3] Corporate governance participants are the board of directors, the audit committee, the top management team, internal auditors, external auditors, and governing bodies, as depicted in Exhibit 6.1.

ROLE OF CORPORATE GOVERNANCE

Corporate governance plays a crucial role in improving the efficiency of the capital market through its impact on corporate operating efficiency and effectiveness, earnings growth, and employment, as well as integrity and quality of financial reports.

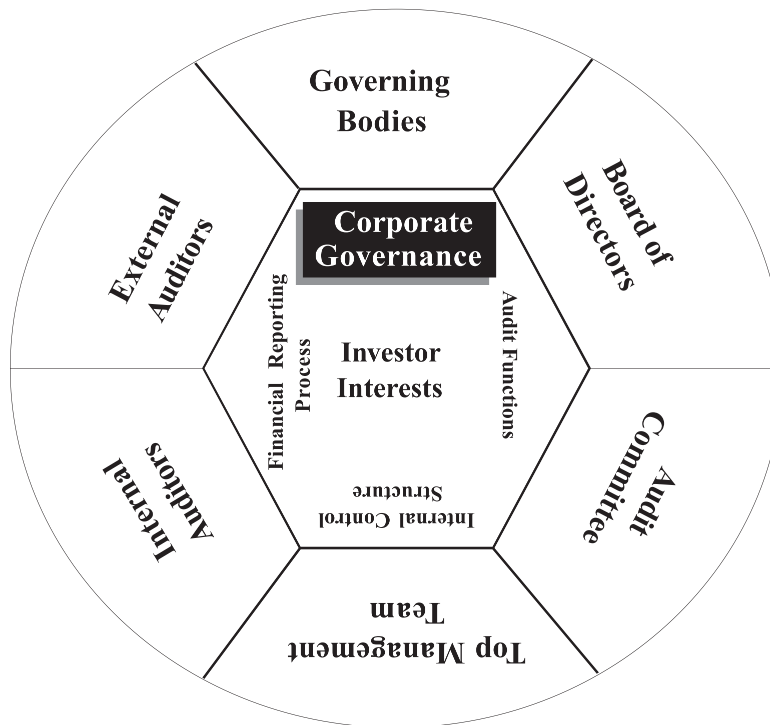


Exhibit 6.1 Corporate Governance and Its Functions

No corporate governance would be necessary if management acted in the best interests of shareholders and if corporate gatekeepers (board of directors, lawyers, and accountants) effectively discharged their fiduciary duties and professional responsibilities. Corporate governance is needed to avoid concentration of power in the hands of management and to create an effective system of checks and balances to appropriately balance power-sharing authority among shareholders, boards of directors, management, and, to a lesser extent, other stakeholders. Corporate governance should monitor the interests of investors and creditors by:

- Assessing the risk associated with their capital investments in the company resources
- Evaluating the allocation of their investment for maximum returns
- Continuously monitoring the administration of their investments

Corporate governance is a monitoring mechanism for assessing corporate responsibility and accountability through boards of directors, audit committees, management, and auditors in order to serve and protect investors.

Corporate governance best practices are centered around the five underlying concepts of accountability, efficiency and effectiveness, integrity and fairness,

responsibility, and equality. The corporate governance structure should ensure that those who manage corporate resources (e.g., management) are monitored and held accountable in using these resources efficiently and effectively. Corporate governance constituencies, in fulfilling their responsibilities, should preserve the integrity and fairness of the corporate governance framework. The corporate governance structure should promote shareholder and societal confidence as well as trust in the corporation's affairs by enhancing the transparency of its financial reporting process, which requires audited financial statements to be free from material errors, irregularities, and fraud and to not be misleading. Thus, responsible corporate governance does five things:

1. It ensures efficient and effective use of corporate resources.
2. It ensures compliance with all applicable laws, regulations, and rules governing corporate affairs and the financial reporting process.
3. It promotes continuous improvements in corporate performance by allowing the best planning for managerial capital acquisition and disbursements.
4. It ensures proper accountability by the board of directors and management as well as effective discharging of their responsibility in achieving the goal of creating shareholder value.
5. It creates trust and confidence in corporate activities by promoting fair relationships between the company and its shareholders and in society at large.

Phar-Mor: Who's to Blame?

Frontline's ''How to Steal $500 Million'' asks the question, ''Mickey (Michael) Monus: crook or classic entrepreneur?''

With financial backing from David Shapiro, Mickey Monus began Phar-Mor in 1982. By 1985, Phar-Mor had 12 stores, and 28 additional stores were open by the end of 1987. As Phar-Mor started to gain momentum, Sam Walton indicated that ''the only company he feared in the expansion of Wal-Mart was Phar-Mor.'' The problem: Phar-Mor increasingly ran into Wal-Mart and began losing money. By 1989, Phar-Mor was losing millions.

To ''buy time,'' Phar-Mor's financial group, headed by Pat Finn, CFO, under the hands-on guidance of Mickey Monus, began to temporarily park losses away from the watchful eye of auditors, investors, and bankers. To conceal the fraud, one of the key Phar-Mor schemes was to hide the losses in inventory. Inventory tracking, management, valuation, and accounting are complex tasks. That complexity makes it an attractive area for fraudsters to exploit. Phar-Mor essentially spread its operating losses across lots of stores and lots of products by slicing the total into small, bite-size pieces. In 1989, Phar-Mor declared record profits, and ''on paper,'' the company continued to grow and prosper.

In July 1991, Corporate Partners invested $200 million into Phar-Mor. The investment was designated for Phar-Mor's growth but actually went to pay old vendor invoices. At about this time, Charity Imbrie, Phar-Mor general counsel, wrote a memo to David Shapiro describing rumors that vendors were refusing to supply inventory because of unpaid bills.

Shapiro indicated that he was aware of issues and that Imbrie should destroy the memo because the content could jeopardize the corporate partners' investment deal.

In spring 1992, the scheme unraveled. By the time the smoke cleared, the Phar-Mor fraud totaled more than $500 million and the scheme had lasted four years. Despite the success it reported in its financial statements, Phar-Mor had not earned any income in five years. On August 17, 1992, Phar-Mor filed for Chapter 11 bankruptcy.

The fallout from this financial statement defalcation was extensive. Worth noting is that everyone claimed to be a victim: the accountants, the auditors, the investors, the chief executive, and the board of directors. All claim it was the other guy's fault.

Mickey Monus was eventually convicted and sentenced to 20 years in prison. Pat Finn, CFO, was sentenced to 33 months, gaining a lighter sentence for his cooperation and testimony against Monus. In the words of Stan Cherelstein: "Don't let it happen . . . Don't let it start. Once you start, it's very easy to let it happen a second time and then, where will it end?"

Source: Jim Gilmore, Paul Judge, and Paul Solman, "How to Steal $500 million," *Frontline*, 1994.

The three corporate governance principles that play a crucial role in preventing and detecting financial statement fraud are:

1. *Transparency*. Ensure financial reports are understandable and that they reflect the economic reality of the company.
2. *Competence and integrity*. The effectiveness of corporate governance depends on the integrity and competence of those who carry out key functional responsibilities (e.g., oversight, managerial, monitoring).
3. *Effective system of checks and balances*. The existence of an effective system of checks and balances ensures proper alignment of interests and division of responsibilities among shareholders, the board of directors, and management.

CORPORATE GOVERNANCE STRUCTURE

Corporate governance is a broad concept consisting of a set of external and internal mechanisms designed to align interests of management with those of shareholders and to ensure compliance with applicable laws, rules, and standards.[4] Corporate governance plays an important role in improving investor confidence in financial reports and capital markets by focusing on three institutional factors:

1. Ownership structure
2. Legal system
3. Capital markets[5]

OWNERSHIP STRUCTURE

Ownership structure is an important aspect of corporate governance that determines the nature and extent of both internal (e.g., composition of the board) and external (e.g., rules and regulations) mechanisms needed to protect investors and minimize the agency costs (e.g., information asymmetries and self-dealing by management). The ownership structure can be either highly dispersed or concentrated. Highly dispersed ownership with significant ownership by institutional investors (e.g., pension funds, mutual funds, insurance companies) is common in the United States and the United Kingdom, and it is usually open to cross-border portfolio holdings.

Concentrated ownership, primarily in the hands of families, is common in Europe and Japan. The agency cost is due to potential conflict between controlling owners and minority shareholders.

LEGAL SYSTEM

The legal system determines the nature and the degree of investor protection across countries due to differences in the legal regime. Two traditional legal regimes influencing corporate governance are civil law and common law.[6] Civil law has its origin in Roman law and is practiced in France, Spain, Italy, Germany, Austria, Greece, Switzerland, Japan, Denmark, Sweden, Norway, and Finland. Common law, which is of English origin, is dominant in Australia, Canada, the United Kingdom, and the United States. The U.S. approach to corporate governance is regarded as a regulatory-led system that provides high standards of protections for investors influenced by policy makers (Congress, SOX), regulators (Securities and Exchange Commission rules), stock exchange listing standards, and state law. These regulations must be cost effective, efficient, and scalable to promote best practices. Any regulatory conflicts or overregulation can have three important effects:

1. Increase compliance costs
2. Have detrimental effects on the long-term attractiveness of U.S. capital markets
3. Cause the markets to have a global competitive disadvantage

For foreign companies, with a low number of U.S. equity shareholders, the compliance costs associated with strict regulations can outweigh the benefits of listing on U.S. capital markets and cause these companies to deregister.

CAPITAL MARKETS

Capital markets are the means through which scarce financial resources are allocated and access to global investments is facilitated. Capital markets provide the forum for global exchanges to list public companies.

Capital markets facilitate the investment process through more efficient allocation of capital, by scrutinizing management and mitigating financial constraints. Taken together, capital markets:

- Enhance investor protection
- Reduce cost of capital
- Improve access to capital
- Strengthen the firm's information environment
- Enhance stock valuation

These benefits are greater for firms in large countries with weak investor protection.

CHARACTERISTICS OF CORPORATE GOVERNANCE

The seven characteristics and attributes of corporate governance most likely to be associated with financial statement fraud are:

1. Aggressiveness
2. Opportunism
3. Cohesiveness
4. Gamesmanship
5. Loyalty
6. Trust
7. Control ineffectiveness

Aggressiveness and opportunism can be signified by the company's attitude and motivations toward beating analysts' forecasts about quarterly earnings or annual earnings per share and the attempt to make Wall Street or its worldwide equivalent happy by reporting a favorable financial performance, whether justified or not. Cohesiveness, gamesmanship, and loyalty attributes create an environment that reduces the likelihood of whistle-blowing and increases the probability of cover-up attempts. Trust and control ineffectiveness can cause those in an oversight function (e.g., board of directors, audit committee) as well as an assurance function (e.g., internal auditors, external auditors) to be less effective in detecting fraud. Cohesiveness and gamesmanship can also cause a sharply defined group boundary of corporate governance that creates high cooperation among corporate governance members in order to conceal financial statement fraud and restrictions leaks of fraudulent financial information to outsiders. This gamesmanship and cohesiveness can encourage more collusion in the development of financial statement fraud. If internal or external auditors discover the fraud, they can cause the company to push the auditors for a cover-up. When the members of corporate governance establish trust, it creates less room for suspicion and skepticism, which in turn may reduce the likelihood of auditors detecting financial statement fraud.

Aldrich Ames: Missing the Clues

Aldrich Ames was convicted in 1994 of spying for the Soviet Union. As a result of his actions, at least 10 persons were believed to be executed by the Russians. What is interesting about Aldrich Ames is all of the clues and red flags that the Central Intelligence Agency (CIA) missed, clues that may have led to earlier detection of Ames's activities. Over an eight-year period, Ames received approximately $2.7 million in cash from the Soviets. His spending of that money was anything but discreet, especially for a person earning a government salary of around $70,000 in 1994:

- He had an upscale home paid with $540,000 in cash.
- He remodeled the home and had lavish landscaping completed.
- He had household servants.
- He had capped teeth.
- He wore expensive Italian suits and shoes.
- He paid $50,000 in cash for a 1992 Jaguar.
- He paid $5,000 per month for phone bills.
- His credit card purchases totaled as much as $30,000 a month.
- He made cash deposits totaling $1.5 million, some of which were reported on Currency Transaction Reports to the Internal Revenue Service.
- He covered a divorce settlement to his first wife.

He explained his activities by claiming that money came from his wife's family. He refused to provide timely accounting and to properly maintain his revolving operational funds. He also used the money laundering techniques of placement, layering, and integration.

Interestingly, the CIA began a financial investigation of Ames in 1989, but it fizzled. The investigation was restarted in 1992 and completed in mid-1993. On February 22, 1994, Aldrich Ames was charged with espionage, conspiracy, and tax evasion. He was eventually convicted and sentenced to life in prison. His wife was also caught up in the activity, being convicted of conspiracy and tax evasion and sentenced to five years in prison.

Ames admitted that the primary motivating factor was his desperate financial situation. He originally conceived of the scam as a one-time activity to earn $50,000. Once started, for Ames like so many others, there was no turning back.

Sources: Wise, David, *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million* (NY: HarperCollins, 1995), excerpted in *Time: Victims of Aldritch Ames*. John Madinger, *Money Laundering: A Guide for Criminal Investigations* (Boca Raton, FL: CRC Taylor and Francis, 2006).

CORPORATE GOVERNANCE FUNCTIONS

The seven essential corporate governance functions are:[7]

1. Oversight
2. Managerial
3. External audit

4. Internal audit
5. Compliance
6. Legal and financial advisory
7. Monitoring

Corporate governance participants fulfill their responsibility when their role in corporate governance is viewed as a value-added function.

OVERSIGHT FUNCTION

The oversight function is granted to the board of directors with the fiduciary duty of overseeing the alignment of the managerial function with the best interests of the company and its shareholders. The effectiveness of the oversight function depends on directors' independence, due process, authority, resources, composition, qualifications, and accountability. The board of directors should provide consultation and advice to management and oversee managerial performance while avoiding micromanaging. The board should perform vigilant and active oversight to be a fiduciary for all stockholders in the corporation. In fulfilling its legal responsibility and requirements, the board of directors should:

- Monitor management plans, decisions, and activities
- Act as an independent leader that takes initiatives to create shareholder value
- Establish guidelines or operational procedures for its own functioning
- Meet periodically without management present to assess company and management performance as well as strategy
- Evaluate its own performance to ensure that the board is independent, professional, and active

MANAGERIAL FUNCTION

Management is given the authority to run the company and manage its resources and operations. The effectiveness of the managerial function depends on the alignment of management's interests with those of shareholders. According to the agency theory, a self-interested top management team manipulates financial reporting by engaging in financial statement fraud to its advantage. Thus, the top management team must be monitored and/or have an appropriate incentive structure. The opportunity to engage in financial statement fraud is influenced by the extent of monitoring done by the company. The motivation is related to the internal corporate environment and those incentives that affect the interest alignment of the top management team with investors and creditors.

EXTERNAL AUDIT FUNCTION

External auditors express an opinion that financial statements truly and fairly represent, in all material respects, the company's financial position and the results of operations in conformity with generally accepted accounting principles (GAAP). External auditors lend credibility to the company's financial reports and thus add value to its corporate governance through their integrated audit of both internal control over financial reporting and of financial statements. In the corporation form of business, ownership is separated from control; thus, it is necessary to monitor the control to ensure that those who have been entrusted with financial resources are being held accountable for their decisions, plans, and actions.

The role of external auditors in corporate governance is to provide assurance that management's financial reports conform to the contractual relationship between the principal (investors and creditors) and the agent (top management team) and are free of material misstatements caused by errors and fraud. Thus, in this context, external auditors monitor financial statements issued by management to users of these reports, especially investors and creditors. Potential investors and creditors are also interested in high-quality, accurate, and reliable financial statements when making further investment decisions. The SEC, in its efforts to protect investors' interests, also requires that financial statements of publicly traded companies be audited by independent auditors to ensure compliance with GAAP and to ensure that published financial statements are free from material misstatements. External auditors add value to the published financial statements by detecting material misstatements that increase the likelihood of financial statement fraud.

Today external auditors are viewed as, and often accused of, not looking hard enough to detect financial statement fraud. They are being challenged and sued for their association with alleged financial statement fraud by aggrieved investors. External auditors have suffered losses, both monetarily and in terms of their reputation, for not properly detecting financial statement fraud. Most recently, on June 19, 2001, the SEC settled enforcement actions against Arthur Andersen, one of the Big Five professional services firms, and four of its current or former partners for their association with the 1992 through 1996 financial statement audits of Waste Management. Arthur Andersen issued unqualified or "clean" opinions on four consecutive years of Waste Management's financial statements, which were misleading because pretax income was overstated by more than $1 billion. The SEC alleged that Arthur Andersen "knowingly and recklessly" issued materially false and misleading audit reports, incorrectly stating that the financial statements were presented fairly, in all material respect, and in conformity with GAAP, and were conducted in accordance with generally accepted auditing standards (GAAS).

INTERNAL AUDIT FUNCTION

The internal audit function provides both assurance and consulting services to the company in the areas of operational efficiency, risk management, internal controls,

financial reporting, and governance processes. Society is concerned about the shock of scandals involving defense contractors, savings and loan associations, banks, and the stock market. Thus, strategies and techniques must be developed to deal with financial statement fraud. Internal auditors are integral parts of corporate governance, and their expertise in internal control is on the front line when it comes to preventing and detecting financial statement fraud.

Internal auditors have been viewed as an important contributory factor in achieving operational efficiency and effectiveness in their organizations. The revised definition of internal auditing specifies that internal auditors' activities are extended to evaluating and improving the effectiveness of a company's governance process. Internal auditing is defined by the Institute of Internal Auditors (IIA) as "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations . . . bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."[8]

COMPLIANCE FUNCTION

This function is composed of a set of laws, regulations, rules, standards, and best practices developed by state and federal legislators, regulators, standard-setting bodies, and professional organizations to create a compliance framework for public companies in which to operate and achieve their goals. Concern over highly publicized audit fraud has prompted several governing organizations to address the problem of financial statement frauds and auditors' failure to detect them.

LEGAL AND FINANCIAL ADVISORY FUNCTION

This function provides legal advice and assists the company, its directors, officers, and employees with complying with applicable laws, regulations, rules, and other legal obligations and fiduciary duties. Financial advisors provide financial advice and planning to the company and its directors, officers, and employees. The function of corporate legal counsel as part of corporate governance has recently received a great deal of attention. Elliot and Willingham[9] argued that two aspects of lawyers' contributions to corporate governance are their obligation to disclose fraud and their relationships to management and boards of directors.

Corporate codes of conduct can be used to encourage ethical and lawful behavior and create an environment that discourages business improprieties. The codes, by establishing appropriate ethical policies and procedures, can spell out the types of behavior and actions prohibited.

MONITORING FUNCTION

This function is exercised by shareholders, particularly institutional shareholders, who are empowered to elect and, if warranted, to remove directors. Shareholders

can influence corporate governance through their proposals and nominations to the board of directors. The influence of shareholder activists on the effectiveness of corporate governance and reliability of financial statements has been controversial. Rule 14a8[10] shareholder proxy proposals are considered ineffective in terms of influencing directors' decisions. Shareholder proxy proposals are not legally binding on the board of directors, as directors usually respond only if they are legally required to do so. Other stakeholders, such as creditors, employees, financial analysts, and investor activists, can also influence corporate policies and practices by being attentive. Shareholders elect directors, and directors appoint officers to manage the company. The effectiveness of the monitoring function depends on company policies regarding shareholder democracy and the engagement of shareholders in corporate governance practices.

GLOBAL CORPORATE GOVERNANCE

There are no globally accepted corporate governance reforms and best practices. Differences are driven mainly by the country's statutes, corporate structures, and culture. Country statutes could pose challenges for regulators in adopting corporate governance reforms and financial reporting disclosures for home companies as well as multinational corporations. The United States and United Kingdom, for example, operate under common law, which tends to give more anti-director privileges to minority shareholders compared to countries under code law (e.g., Germany); under common law, regulators allow too many rights to minority shareholders, whereas under code law, regulators allow too few rights to minority shareholders. Another example is that regulations in the United States are typically regulator-led, being established by the SEC to protect investors; reforms in the United Kingdom are normally shareholder-led (investors are responsible when it comes to safeguarding their own interests).[11]

Corporate and capital structure can also influence corporate governance and financial disclosure requirements. One of the key differences in corporate structure is company ownership. In the United States, ownership of shares is dispersed, as more than 100 million Americans own shares in companies through direct investment and retirement plans. Comparative stock ownerships in Europe are more concentrated; thus, controlling shareholders are in a better position to influence corporate governance and business operations. Corporate governance in a dispersed share ownership is designed to align interests of management with those shareholders, as management may have incentives to engage in earnings management and focus on short-term considerations at the expense of sustainable shareholder value creation and long-term performance. Conversely, with a concentrated ownership, corporate governance creates a right balance between interests of minority and majority shareholders. The primary purpose of corporate governance in the United States is to enhance shareholder value creation while protecting interests of other stakeholders (creditors, employees, suppliers, customers, government); in Germany, the focus is more on protecting creditors, as banks play an important role in financing companies.

The board system can also influence corporate governance. In one-tier boards in the United States, directors are elected to oversee management in running the company; in the two-tier board system in Germany, the supervisory board advises, appoints, and supervises the management board in managing the operation of the company. Japan's companies operate through a complex system of committees, which oversee and run the company. Cultural and political differences can also influence corporate governance, as some cultures are more collective and risk averse than others (e.g., Germany compared to the United States).

An appropriate question is whether these differences in corporate governance can be reconciled and whether convergence in corporate governance is possible. A move toward corporate governance integration was attempted in 1999 by the Organization for Economic Cooperation and Development.[12] It has established a set of corporate governance principles, which were later adopted by the International Corporate Governance Network (ICGN) and were designed to protect all stakeholders, particularly shareholders.

Corporate governance models throughout the world can be classified into three general categories: close, open, and hybrid. The close model of corporate governance has eight characteristics:

1. Concentration of ownership of both equity capital and debt capital
2. A long-term financing relationship with a few borrowers and lenders
3. Less dependence on capital markets for financing activities
4. More direct control and management by a few major investors such as banks, insurance, or individuals
5. More direct and close oversight function by monitoring bodies such as supervisory boards
6. A well-balanced distribution of control rights and information rights
7. Less information asymmetry between management, the supervisory board, and major investors
8. More focus on internal information flows and controls

An example of a close model, which is also referred to as ''insider control,'' is German corporate governance.

The open model of corporate governance, better known as the ''market based'' or ''outsider'' model, has these eight characteristics:

1. Total reliance on capital markets for sources of financing activities (both equity capital and debt capital)
2. Less concentration of ownership in the hands of a few major investors
3. An oversight function by the board of directors
4. Less regulation of corporate governance and corporate activities

5. Total separation of the managerial function and oversight function
6. Existence of a market-based system of checks and balances
7. Information asymmetry between management, the board of directors, and investors
8. More focus on external information flows and controls

The hybrid model focuses on protecting interests of all stakeholders, including investors, creditors, employees, customers, suppliers, government, and society. The eight primary aspects of corporate governance under this model pertaining to the board of directors are:

1. A single board that is collectively responsible for the success of the company
2. Separation of the position of the CEO and the chairperson of the board
3. A proper balance of independent and inside directors
4. Strong independent board committees (audit, compensation, governance, nomination)
5. Emphasis on objectivity of directors in the interests of the company
6. Transparency on appointments and compensation of senior executives
7. Annual evaluation of directors' and officers' performance
8. Effective rights for shareholders in the election of directors and approval of the appointment of senior executives

ANTIFRAUD APPLICATIONS FOR PRACTICE

An outline of the basics of fraud risk management for those charged with corporate governance—the board of directors, audit committee, management, internal, and external auditors—is presented next. With regard to corporate malfeasance, fraud risk management must include five key features:[13]

1. A written policy that outlines the fraud risk management program
2. Targeted fraud risk assessment of the organization's exposure to potential schemes that need to be mitigated
3. Prevention techniques
4. Detection techniques, which are in place:
   - In case preventive measures fail
   - To address unmitigated risks (where the cost of mitigation exceeds the benefits)
   - To address concerns over collusion and management override
5. A reporting process

The written fraud risk management policy should assign and outline these roles and responsibilities:

- Oversight of fraud risk management (board of directors/designee)
- The design and implementation of the fraud risk management program (management)
- The key roles and responsibilities of these participants with respect to fraud:
  - Board of directors
  - Audit committee
  - Executive and senior management
  - Internal audit
  - Management/supervisory staff
  - Staff/line employees

The goals of the fraud risk management program typically include:

- Assessing risk exposure
- Ensuring compliance with policies and procedures
- Identifying and investigating allegations
- Reporting on the effectiveness of the program
- Providing a supportive culture

The written fraud risk management program should include an organizational commitment to an antifraud culture and environment that includes:

- Recognition and awareness of fraud's existence
- Affirmation by all employees, vendors, suppliers, and customers that they are aware of and understand the entity's positions, policies, and responsibilities with respect to fraud
- A commitment to the disclosure of conflicts of interest
- Recognition of the options to deal with those in violation of policies and procedures: termination of (the individual, activity, or association with a third-party entity) and of the implications (e.g., negative impact on the organization's reputation), as well as a commitment to ensure implications do not arise
- A commitment to complete a (targeted) fraud risk assessment
- A commitment to reporting procedures
- A commitment to whistle-blower protections

The written fraud risk management program should address these areas concerning the investigative process:

- Who will investigate (e.g., when to call in outsiders versus conducting an internal investigation)
- Recognition of investigation issues, such as rules of evidence, chain of custody, and the rights of individuals
- Recognition of and compliance with regulatory and legal requirements

The written fraud risk management program should establish the need for remedial action:

- Consequences:
  - For those who commit corporate malfeasance (e.g., termination, civil or criminal action)
  - For those who condone corporate malfeasance (e.g., do not report)
- Postmortem:
  - How did it happen?
  - How did we miss it?
  - Should we attempt to prevent it in the future?

Finally, the written fraud risk management program should address the need for periodic performance (effectiveness) measurement and a commitment to continuous monitoring. Performance measurement can be completed by:

- Creating and monitoring of descriptive statistics
- Benchmarking against other organizations
- Surveying employees, customers, vendors, suppliers, and others

The last thought:

> *Trust but verify.*
>
> —Ronald Reagan

NOTES

1. "Suspending Indictment alleging additional bank fraud charges returned against lawyer in connection with refco fraud." Southern District of New York, December 4, 2008; available at www.usdoj.gov/usao/nys/pressreleases/December08/collinsjosephrefcos1indictmentpr.pdf.
2. Emergency Economic Stabilization Act 2008; available at frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h1424enr.txt.pdf.
3. Zabihollah Rezaee, *Corporate Governance Post-Sarbanes-Oxley. Regulations, Requirements and Integrated Processes* (Hoboken, NJ: John Wiley & Sons, 2007).

4. Much of discussion in this section is from Zabihollah Rezaee, *Corporate Governance and Ethics* (Hoboken, NJ: John Wiley & Sons, 2008).
5. M. S. Beasely, J. V. Carcello, and D. R. Hermanson, *Fraudulent Financial Reporting: 1987–1997. An Analysis of U.S. Public Companies*, Research Commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (Jersey City, NJ: COSO, 1999).
6. Zabihollah Rezaee, *Corporate Governance Post-Sarbanes-Oxley. Regulations, Requirements and Integrated Processes* (Hoboken, NJ: John Wiley & Sons, 2007).
7. Ibid.
8. IIA, ‘‘Definition of Internal Auditing: IIA Practices Framework,’’ 2007; available at www.theiia.org.
9. R. K. Elliot and J. J. Willingham, *Management Fraud: Detection and Deterrence* (New York: Petrocelli Books, 1980).
10. Rule 14a-8 – Proposal of Security Holders (general rules and regulations promulgated under Securities Exchange Act of 1934); available at www.law.uc.edu/CCL/34ActRls/rule14a-8.html.
11. Much of the discussion in this section is from Zabihollah Rezaee, *Corporate Governance and Ethics* (Hoboken, NJ: John Wiley & Sons, 2008).
12. ‘‘OECD Principles of Corporate Governance,’’ 1999; available at http://www.bestpractices.cz/praktiky/ETIKA_V_PODNIKANI/p2003_oecd_principles_of_corporate_governance.pdf.
13. IIA, AICPA, and ACFE, ‘‘Managing the Business Risk of Fraud: A Practical Guide’’ (2008); available at www.acfe.com/documents/managing-business-risk.pdf.

Chapter 7

Board of Directors' Oversight Responsibility

INTRODUCTION

To date, more than 250 public companies have been probed for alleged stock option backdating. The board of directors, with its responsibility to shareholders, is in a unique position to identify and evaluate important policies, procedures, and practices proposed by executive management. Traditionally, regulators have not been aggressive in bringing charges against directors of fraud-prone companies, such as Enron, WorldCom, Adelphia, Qwest, and Global Crossing. It is very rare that outside directors serving on board committees come under scrutiny and investigations by federal authorities for their decisions on the board. However, a vigilant and effective board of directors can play an important role in ensuring the quality, integrity, and reliability of business and financial reports. In overseeing the financial reporting process, the board of directors can prevent and detect financial statement fraud. The passage of the Sarbanes-Oxley Act (SOX) of 2002 has changed the structure and composition of public company board of directors. This chapter examines the role of the board of directors: its composition, functions, attributes, and monitoring role in preventing and detecting financial statement fraud.

ROLE OF THE BOARD OF DIRECTORS

The role of the board of directors in corporate America can be best described as a mechanism for preventing the concentration of power in the hands of a small group of top managers and for creating a system of checks and balances in corporations through its authority, given by shareholders, to hire management and monitor management plans, decisions, and actions. The separation of ownership and control in corporations requires the board of directors to:

- Harmonize manager-shareholder (agency) conflicts of interest
- Safeguard invested capital
- Approve management decisions
- Assess managerial performance
- Allocate rewards in manners that encourage shareholder value creation

Thus, the effectiveness of the board of directors depends significantly on its independence from the top management team. However, management, through its power to nominate or even select directors, can dominate the board of directors and diminish the board's effectiveness in monitoring management.

The board of directors, as an important internal component of corporate governance, receives its authority and responsibility from shareholders who use their voting rights to elect board members. The board of directors assumes the responsibility to oversee and monitor managerial decisions and actions. Separation of ownership from the decision-making process, coupled with the risk-diversification strategy of stockholders to invest in securities of numerous firms, causes owners to delegate their authority and decision control to the board of directors. The board delegates its decision-making authority to management, which makes decisions on a day-to-day basis on behalf of shareholders. Furthermore, shareholders, as residual and risk-bearing claimants in corporations, are not involved in the day-to-day decision-making process. Accordingly, decision functions are separated from risk-bearing, residual claimants. This separation, along with the lack of an adequate incentive and/or costly process for shareholders to be involved in decision control, causes stockholders to elect the board of directors as the internal corporate governance responsible for managerial decision control. Although the board of directors usually delegates its decision functions to management, it retains its decision control and monitoring function by:

- Monitoring managerial decision functions
- Overseeing the adequacy and effectiveness of internal control systems
- Overseeing the effectiveness of audit functions
- Overseeing the integrity, reliability, and quality of the financial reporting process

This is depicted in Exhibit 7.1.

The board of directors' primary responsibility as the gatekeeper and ultimate internal control mechanism is to protect interests of all stakeholders, including shareholders, by minimizing management expropriation of shareholder wealth through financial statement fraud. The board is in a unique position and has the ultimate responsibility to monitor management decisions or actions. However, financial statement fraud can occur when management acts in its own self-interest and fraudulently to issue materially misleading financial statements and the board of directors fails to monitor management actions, oversee the internal controls structure and financial reporting process, and prevent and detect financial statement fraud.

COMPOSITION OF THE BOARD OF DIRECTORS

The board of directors typically is composed of both internal members (e.g., top managers) and external members (e.g., outside, nonemployees). Inside members of the board typically have the ability and experience of using inside information;

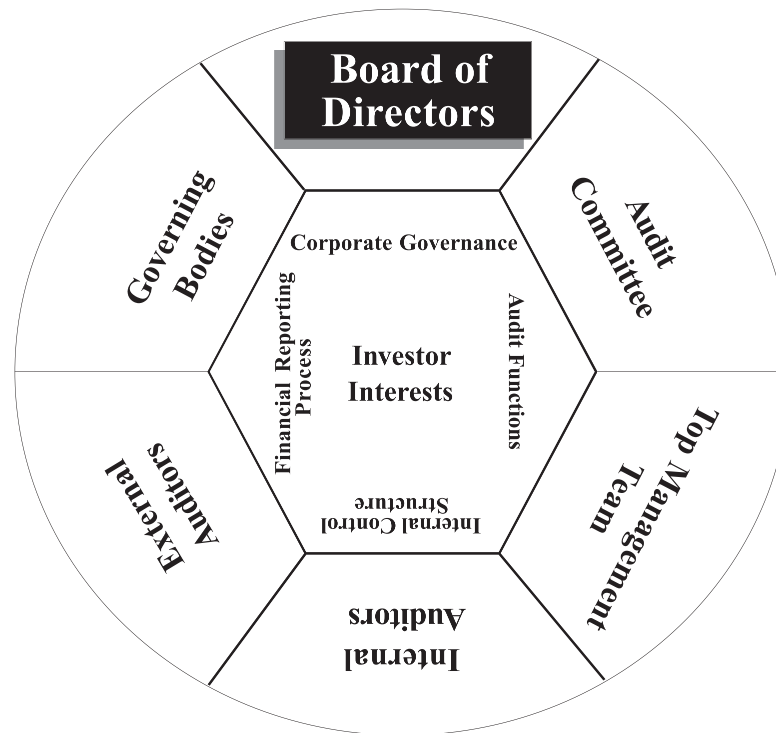


Exhibit 7.1 Corporate Governance and Its Functions

their full-time status and inside knowledge may enhance the quality and quantity of information coming from internal monitoring systems. Outside members, however, can be more independent in exercising their authority to monitor management decisions and actions.

The effectiveness of the board as a monitor of management depends on the quality, reputation, and independence of board members. The presence of outsiders on the board gives the appearance of board independence, but its effectiveness is measured based on the quality of its membership. There are some variations in director fiduciary duties as company law differs from one state to another. However, directors are empowered to manage the affairs of a company, and directors must exercise their powers in the best interests of the company and its shareholders. In fulfilling their fiduciary duties of care and loyalty, directors are governed by the business judgment rules of exercising their best judgments when aligning management interests with those of shareholders and when creating shareholder value. The business judgment rule is intended to protect directors from undue liability when making business decisions in good faith and in the best interests of the company and its shareholders. The majority of directors in the post-SOX period should be independent, nonexecutive directors who work collectively with chief executive officers (CEOs) in the best interests of the company and its shareholders. The primary responsibility of the board is to hire a

competent and ethical management team to run the company effectively. Executive directors typically are engaged in strategic decision making, planning, and execution of plans; nonexecutive directors advise and oversee managerial plans, decisions, and actions without micromanaging.

Stock Options Backdating, the Story Continues . . .

Backdating of employee stock options is not necessarily illegal if these conditions hold:

- No documents have been forged.
- Backdating is clearly communicated to the company's shareholders.
- Backdating is properly reflected in earnings.
- Backdating is properly reflected in taxes.

Unfortunately, in the backdating scandals in the 2000s, these conditions were rarely met, making backdating of grants illegal in most cases.

The mysterious timing of stock options has been a subject of academic research since the 1990s. Initially, Yermack and Aboody and Kasnik assumed that the timing (dating) of stock options was oriented around good news and bad news. In 2004, Lie suggested that the timing was set to exploit marketwide price depressions that no one, including insiders, could predict, leading to a conclusion that at least some of the option grants were retroactive. The backdating scandal has publicly ensnared as many as 250 public companies and is estimated to cost more than $10 billion. Given that most frauds are one-time events, relatively unique activities affecting a single organization, one might ask: How did such an illegal practice get started?

We see epidemics more frequently than one might hope:

- The 2007–2008 subprime mortgage crisis will cost Americans trillions of dollars. Although fraud is not considered a major cause at this time, a failure of corporate leadership to properly evaluate the risks associated with their business practices was an inherent issue.
- Prior to the current mortgage crisis, in the early 1980s, the American public suffered through and paid for the savings and loan crisis. During that crisis, an estimated 1,700 savings institutions and almost 500 thrifts failed.

So where do corporate governance leaders get ideas that may lead to fraudulent actions and unsound business practices? The answer is not obvious, but once a practice, even an illegal one, becomes trendy, it creates pressure on companies competing for the same managerial talent, the same stock price appreciations, and the same customers to at least consider doing the same.

Sources: "Backdating of Executive Stock Option (ESO) Grants," available at www.biz.uiowa.edu/faculty/elie/backdating.htm. David Yermack, "Good Timing: CEO Stock Option Awards and Company News Announcements," *Journal of Finance* (June 1997). David Aboody and Ron Kasznik, "CEO Stock Option Awards and the Timing of Corporate Voluntary Disclosures," *Journal of Accounting and Economics* (February 2000). Erik Lie, "On the Timing of CEO Stock Option Awards," *Management Science* Vol. 51, No. 5, May 2005, pp. 802–812. Mark Hulbert, "Why Backdated Options Might Be Contagious," *New York Times*, January 21, 2007.

FUNCTIONS OF THE BOARD OF DIRECTORS

Responsible corporate governance requires that the business of a corporation be conducted under the direction of the board of directors, where the board may delegate to management the authority and responsibility to manage the daily affairs of the corporation. Under an ideal corporate governance structure, the board of directors is able to create shareholder value while its oversight functions ensure proper accountability for managerial decisions and activities. The primary functions of the board, as stated in the Statement on Corporate Governance of the Business Roundtable, are the following:

- Select, regularly evaluate, and, if necessary, replace the chief executive officer; determine management compensation; and review succession planning
- Review and, where appropriate, approve the major strategies and financial and other objectives as well as plans of the corporation
- Advise management on significant issues facing the corporation
- Oversee processes for evaluating the adequacy of internal controls, risk management, financial reporting, and compliance, and satisfy itself as to the adequacy of such processes
- Nominate directors and ensure that the structure and practices of the board provide for sound corporate governance[1]

Corporate boards, through vigilant oversight of the company's governance, financial reporting, and audit activities, can significantly reduce the likelihood of the occurrences of financial statement fraud. The board should oversee the financial reporting process to ensure that management has effectively carried out its financial and internal control reporting. This oversight function by the board of directors and its representative audit committee is particularly essential because controls are designed and performed by management, subject to management override, and often cannot be monitored objectively by management. The board should also oversee the entire financial reporting process to evaluate the fair and true presentation of financial statements and obtain an understanding of how management has met its financial and internal control reporting responsibilities. Thus, the board of directors should have reasonable assurance that management and external auditors are meeting their responsibilities in ensuring the integrity, quality, reliability, accuracy, and completeness of financial reports. The results of a recent survey suggest that even more than five years after the passage of SOX, many corporate board members do not appear to serve the shareholders whom they are representing. More than 13 percent (45 percent) of surveyed financial advisors and 12 percent (43 percent) of high-net-worth investors (those with $1 million or more investable assets) felt that corporate governance practices have improved a great deal (a moderate amount) in the post-SOX era.[2] This suggests that investor confidence in corporate governance after the post-SOX period is not significantly improved. However, there appears to

be a strong association between corporate governance and corporate reputation. Furthermore, 82 percent of advisors and 71 percent of investors believe reputation accounts for 20 percent of a company's share value. Fifty-six percent of financial advisors and 41 percent of investors feel that a board accounts for more than 10 percent of a company's market value.

PricewaterhouseCoopers in its 2007 publication *Global Best Practices: Building Blocks of Effective Corporate Boards* discusses eight attributes that assist directors in creating an appropriate balance between their role as compliance watchdogs and that of participating in managerial strategic planning, thus effectively overseeing the financial reporting process:[3]

1. *Create an open and engaging boardroom atmosphere*. Effective boards are those whose directors work well in teams, possess good listening and problem-solving skills, have the diverse experience to address relevant business and industry issues, and are independent-minded. Directors should advise management in strategic planning without micromanaging and oversee management operational, compliance, and reporting functions, including internal control over financial reporting.
2. *Maximize the value of the board's time commitment by establishing clear roles and responsibilities within an appropriate structure*. To be effective, directors should focus their efforts on the most relevant and important issues that contribute to the achievement of sustainable performance in creating shareholder value.
3. *Determine the information the board needs and ensure it is delivered on a timely basis*. The company's board should receive the right information in the right format and at the right time to fulfill its oversight function effectively. In particular, the board's audit committee should receive adequate information about the company's internal control and financial reports, risk assessment, and compliance reports.
4. *Dedicate time to strategic issues*. The board of directors should be proactively engaged with management in establishing strategic planning, setting strategic priorities, and executing these priorities in a timely manner.
5. *Create a transparent, explicit, and accountable executive pay process*. Executive compensation should be linked to the company's long-term sustainable performance and aligned with the market and peer groups' benchmarks. It should also pass the commonsense test in the public eye and be transparent.
6. *Actively engage in the CEO succession process*. The board of directors should plan and be committed to the CEO succession process for replacement of a CEO in case of crisis and establish CEO selection criteria for a successor under normal circumstances.
7. *Assess the strength of the company's management talent*. The management team, led by the CEO, is crucial in ensuring the effectiveness of corporate

governance and long-term sustainable shareholder value creation. The board of directors should ensure that the company has committed adequate resources to attract, train, and retain a competent and ethical management team.

8. *Monitor the company's enterprise risk management system*. The board of directors should oversee the adequacy and effectiveness of the company's risk management system. Some companies have established a position of chief risk officer (CRO) to coordinate risk management activities among the board of directors, management, and key personnel. The CRO, under the direct oversight of the board of directors and close cooperation with senior executives (CEO, CFO), should establish the strategy for the company's risk management, provide guidance for the proper implementation of the strategy, and review the implementation of the guidance.

The UK Companies Act of 2006 provides more prescriptive duties of directors, which require them to act in good faith in the best interests of the company in such a way that promotes the success of the company for the benefit of its shareholders.[4] Specifically, directors have seven general duties:

1. *Duty to act within powers*. Directors must act in accordance with the company's constitution and exercise their powers for the purposes for which they are conferred.
2. *Duty to promote the success of the company*. Directors must act in good faith to promote the success of the company for all of its shareholders. In effectively fulfilling this duty, a director must consider:
   - The likely consequences of any decision in the long term
   - The interest of the company's employees
   - The need to foster the company's business relations with its stakeholders, including suppliers and customers
   - The effects of the company's operations on the community and the environment
   - The company's reputation of high standards of business conduct and fairness
3. *Duty to exercise independent judgment*. Directors must exercise independent judgment in fulfilling their duties.
4. *Duty to exercise reasonable core, skill, and diligence*. Directors must exercise the core, skill, and diligence expected of a reasonable and diligent person.
5. *Duty to avoid conflicts of interest*. Directors should avoid situations and opportunities that may conflict with the interests of their company.
6. *Duty not to accept benefits from third parties*. Directors must not accept benefits from any person other than their company when acting on the company's behalf.

7. *Duty to declare interest in proposed transactions or agreements*. Directors must disclose the nature and extent of their interest in their company to the other directors.

Sam Walton Protégé Pleads "Guilty"

Thomas M. Coughlin celebrated the beginnings of 2005 as a board member and the vice chairman of Wal-Mart. Coughlin was a legend inside the company. In 1978, Thomas Coughlin was hired as director of loss prevention. The pinnacle of Coughlin's career came as vice chairman of Wal-Mart Stores, Inc. He was a personal friend of Wal-Mart founder and entrepreneur extraordinaire Sam Walton.

On January 24, 2005, Coughlin resigned from Wal-Mart's board of directors among allegations of fraud and deceit. Documents reviewed by the *Wall Street Journal* "suggest that Mr. Coughlin periodically had subordinates create fake invoices to get Wal-Mart to pay for his personal expenses. The questionable activity appears to involve dozens of transactions over more than five years, including hunting vacations, a $1,359 pair of alligator boots custom made for Mr. Coughlin and a $2,590 dog pen for Mr. Coughlin's Arkansas home." According to the article, Wal-Mart found questionable transactions totaling between $100,000 and $500,000. While he faced more than 28 years in prison and fines of $1.35 million, the judge opted for 27 months of home detention, five years of probation, and 1,500 hours of community service. He also fined Coughlin $50,000 and ordered him to pay $411,218 in restitution.

Here's the kicker: In the year immediately prior to his resignation, Mr. Coughlin's compensation totaled more than $6 million.

Sources: James Bandler and Ann Zimmerman, "A Wal-Mart Legend's Trail of Deceit," *Wall Street Journal*, April 5, 2005. Allison Grant, "Former Wal-MART Exec Thomas Coughlin Resentenced to Home Detention," *The Plain Dealer* (Cleveland.com) February 1, 2008. Brian White, "Former Wal-Mart Manager Sues Tom Coughlin—for Her Own Misdeeds," *Blogging Stocks*, April 1, 2008, available at www.bloggingstocks.com/2008/04/01/former-wal-mart-manager-sues-tom-coughlin-for-her-own-misdeeds.

ATTRIBUTES OF BOARDS OF DIRECTORS

STOCK OWNERSHIP

Empirical studies of stock ownership[5] provide evidence indicating that the firm's owners have an incentive to prevent financial statement fraud to protect their investment. These studies conclude that as the percentage of ownership by directors increases, the probability of financial statement fraud decreases. The effective monitoring of management decisions and actions to minimize the probability of financial statement fraud requires adequate time and effort. Thus, financial interest in the company provides incentives for outside directors to fulfill their responsibility of monitoring managerial decisions more effectively. Directors with sizable ownership interest in a firm or control over a large block of votes are more likely to

question and challenge management decisions and to monitor management closely to prevent financial statement fraud. A higher percentage of ownership in a firm's outstanding equity should provide individual directors with a strong incentive to promote activities that create shareholder value, which in turn increase the value of the directors' investments. Thus, as the extent of ownership interests of outside directors increases, the probability of financial statement fraud should decrease.

Empirical research has found that outside directors who hold ownership interest and receive stock-based compensation typically are motivated to monitor the top-level management team, including CEOs, and become more involved with the company's operation and financial reporting process.[6] As the stock ownership by outside directors increases, however, the probability that a firm's CEO and other top managers will attempt to exert control over these outside directors increases. This concern was addressed in Cadbury's report in the United Kingdom, which prohibits outside directors from holding strong equity positions in their firms.[7] Although this concern is not currently deemed serious in the United States, when companies increase their use of stock ownership as a means of motivating outside directors, the independence, objectivity, and effectiveness of these directors in monitoring management may be compromised.

LEADERSHIP OF THE BOARD OF DIRECTORS

The leadership of the board of directors can be unitary or dual. The leadership is dual when the role of the CEO is separated from that of the chair of the board of directors. Unitary leadership exists when one individual holds both the position of the CEO and the chair of the board. Corporate governance can be improved under dual leadership of the board because the individual who chairs the board is expected to exercise significant influence over the board's activities. When unitary leadership exists, the interests of shareholders are likely to be compromised. Prior research[8] concludes that companies that engage in financial statement fraud typically have the CEO as the board chair. One of the most controversial and unresolved issues in corporate governance worldwide, particularly in the United States, has been CEO duality. No rules, regulations, or standards in the United States require the separation of functions of the CEO and the chair of the board. Corporate governance reforms in other countries (e.g., the United Kingdom) do promote the separation of the two positions. Best practices recommend the separation of the positions in those cases where the CEO can influence the nomination of independent directors and has the ability and the tendency to dominate the board leadership and process.

In cases where CEO duality exists, the lead director should be in charge of managing as well as running the board.

DIRECTOR ACCOUNTABILITY AND PERSONAL LIABILITY

Recent corporate governance reforms, including SOX, have not adequately tackled director liability or accountability. In some cases, directors are paying out of their

pockets for their breach of fiduciary duties (former Enron's directors), and shareholder class action lawsuits are often settled out of the court before trial. Settlements are usually paid by companies or their directors' and officers' liability (D&O) insurance. Ultimately, shareholders bear the costs of director litigation, which eventually dilutes the value of their shares. Ten former Enron directors agreed to pay $13 million out of their own pockets as part of a $168 million settlement of a shareholder-filed lawsuit, with the remainder of the settlement being paid by D&O insurance policies. The prescriptive approach used in the UK Companies Act of 2006 in specifying directors' duties along with the higher standard of skill, care, and due diligence expected of directors could expose directors of UK companies to a greater risk of liability.[9] To mitigate such a risk, the act allows UK companies to agree to indemnify directors against claims and liabilities resulting from negligence, default, and breach of duty, including associated legal costs brought by third parties or unsuccessful claims brought by the company. Nonetheless, directors usually are not released from such claims and cannot be protected against criminal liability and liabilities owed to the company. Companies are allowed to buy directors' and officers' liability insurance for the benefit of directors.[10] Despite all the lawsuits brought against directors on the board for not fulfilling their monitoring management responsibility, their accountability remains questionable.

NOMINATION PROCESS

Regulations in the United States, including SEC rules, do not grant shareholders the right to place the names of director-nominees or even resolutions regarding the election process on the corporate ballot, whereas management uses the company's assets (shareholder residual claims) to distribute those ballots to campaign for its candidates. Pfizer, on June 28, 2007, announced that its board of directors will have face-to-face meetings with the company's institutional investors on corporate governance policies and practices.[11] Pfizer is the first public company to initiate such meetings, which provide an opportunity for institutional investors to offer comments and perspectives on the company's governance policies and practices, including executive compensation. Ten other Pfizer corporate governance best practices are listed next:

1. Shareholders have better access to the lead director and board committee chairs through e-mail.
2. The board has a policy of regularly reviewing communications received from shareholders.
3. Directors regularly participate in investor conferences relevant to governance practices.
4. The poison pill has been eliminated.
5. The board has been declassified.
6. A majority-voting policy has been adopted.

7. Additional disclosures are required regarding executive compensation above and beyond the SEC disclosure requirements.
8. ‘‘Plain English’’ rules are used to make disclosures more understandable to investors.
9. Open and candid communications have been established with shareholders.
10. All stakeholders’ viewpoints on governance are addressed, including those of shareholders, employees, customers, suppliers, and government.

VOTING SYSTEM

The election of directors is a vital role of the shareholders in corporate governance, as directors serve as agents. Under plurality voting, only one ‘‘for’’ vote will ensure the candidate’s seat on the board regardless of the number of ‘‘withheld’’ or ‘‘against’’ votes. This method may work fairly when there are more candidates than available board seats, but it can be ineffective when the candidate is ensured approval with as little as one vote. Majority voting empowers shareholders by requiring that the candidate be elected through approval from a majority of shareholders.

Under the plurality voting system, directors encounter few, if any, challenges and little chance of losing an election. Academic research suggests that directors usually do not suffer reputational damages from low votes, as the lower number of votes has no effect on their appointment or any change in firm governance or performance.[12] Nonetheless, directors who attended less than 75 percent of board meetings or received a negative Institutional Shareholder Services (ISS) recommendation obtained 15 percent and 18 percent fewer votes, respectively.[13]

DIRECTOR INDEPENDENCE

The SEC rules require that companies identify and disclose the independent directors and director nominees as determined by the definition of independence in their applicable listing standards (e.g., New York Stock Exchange, NASDAQ). Public companies should also disclose any members of their audit, compensation, and nominating committee who are not independent. The SEC requires four disclosures:

1. Disclosure of whether each director and director nominee is independent
2. A description of any transactions, relationships, or arrangements not disclosed or a related person transaction that was considered by the company’s board of directors when determining whether applicable independence standards were met
3. Disclosure of any audit, nominating, and compensation committee members who are not independent
4. Disclosure regarding the compensation committee’s processes and procedures for considering compensation of the company’s directors and executives[14]

One example of violation of director independence is when the board chairwoman, Patricia C. Dunn, at Hewlett-Packard Co., ordered investigators to spy on the outside directors who may have leaked confidential information to reporters.[15] Investigators used deception to obtain confidential records by lying to obtain telephone records of directors and reporters. To prevent further occurrence of eavesdropping or spying in the form of pretexting on directors who dissent or even vote the wrong way, boards should promise directors that they will not seek access to directors' confidential telephone or other records without written permission. The board of directors should set an appropriate tone at the top that promotes ethical and legal behavior throughout the company. Any attempt to spy on directors is not only unethical and potentially illegal but also violates director independence.

DIRECTORS' EMERGING ISSUES

Eight post-SOX improvements in the structure of many public company boards of directors are listed here:

1. Many boards have moved beyond mere compliance with applicable regulations and now engage more proactively in independent stewardship and accountability.
2. The overall makeup of boards is more independent. More than 40 percent of boards have only one nonindependent director (the CEO), and the median number of inside directors is two compared with four, which was the standard nearly 20 years ago.
3. All mandatory board committees (audit, compensation, and nomination/governance) are composed of independent directors.
4. The supermajority (94 percent) of boards has designated an independent lead or presiding director to improve the independence of board leadership.
5. The lead or presiding director has made independent directors more accountable for and vested in oversight functions.
6. Boards of directors have addressed the issue of CEO succession more proactively.
7. Institutional investors are more engaged in effective monitoring of corporations by approaching the board directly to voice their governance concerns.
8. Some boards have implemented best practices of corporate governance above and beyond mere compliance with rules and regulations (e.g., change to majority voting systems).

Directors' emerging issues include director liability, accountability, role in crisis management, and executive compensation.

Establishing appropriate executive compensation that aligns executives' interests with those of shareholders and links executive pay with performance is perhaps

the most profound challenge facing many boards. Director accountability and related liability is the second most important challenge for directors. Finally, directors' ability and willingness to deal effectively with executive departures, succession planning, and crisis management are also important challenges.

A summary of the challenges are:

- Director accountability and liability
- The separation of the roles of board chair and CEO
- Executive compensation
- Board diversity

BOARD COMMITTEES

The entire board of directors is responsible for acting in the best interest of the company's shareholders and for protecting the interests of other stakeholders. To fulfill its responsibility effectively, boards of directors perform their oversight function through well-structured committees. Corporate governance reforms, including SOX, listing standards of national exchanges, and best practices, recommend public companies establish at least three board committees:

1. The audit committee, composed of at least three independent directors
2. The compensation committee, composed of at least three independent directors
3. The nominating committee, composed of at least three independent directors

Public companies may also form other special committees (e.g., governance, finance, budget, mergers, and acquisition) to address special board projects, as needed. The chair of each committee should present the committee's findings and recommendations to the entire board for approval and action. The audit committee's roles and responsibilities in preventing and detecting financial statement fraud are discussed thoroughly in Chapter 8. The following paragraphs summarize the function of the compensation and nomination committees normally formed by public companies.

COMPENSATION COMMITTEE

The compensation committee generally is formed to determine the compensation and benefits of directors and executives. The role of the compensation committee has received great attention during the recent debate on outsize compensation for top executives of financial institutions and banks whose bad decisions caused the mortgage crisis and the resulting 2008–2009 meltdown on Wall Street. To be effective and objective, the compensation committee should be composed of independent outside directors with sufficient human resources experience in compensation and related issues.

SEC rules require public companies to describe their compensation committee's processes and procedures, including:

- The scope of authority of the compensation committee
- The nature and extent of the authority that is being delegated by the compensation committee to other persons
- Any role that compensation consultants play in determining or recommending the amount or form of executive and director compensation

This information regarding compensation consultants should be disclosed:

- The name of each consultant
- Whether the consultants were engaged and retained directly by the compensation committee
- The nature, extent, and scope of the consultants' assignment
- The extent and nature of guidelines and instructions given to the consultants regarding their responsibilities and performance

NOMINATING COMMITTEE

The nominating committee is responsible for nominating a new director to the board. It also facilitates shareholders' election of a new director. The committee may use staffing support to identify and recruit new members of the company's board. An effective nominating committee can substantially reduce the traditional role played by the CEO in selecting new directors who may not be independent from management. The nominating committee typically evaluates the performance of the existing directors and nominates their reelection for shareholder approval.

ANTIFRAUD APPLICATIONS FOR PRACTICE

According to "Managing the Business Risk of Fraud: A Practical Guide," the roles and responsibilities of the board of directors with regard to fraud can be summarized in this way: [16]

- Be independent minded
- Set its own agenda
- Make fraud prevention, deterrence, and detection a periodic agenda item
- Maintain control over the sources and flow of information it needs to complete its work
- Maintain access to management and employees: financial and operational personnel

- Encourage ethical behavior and act accordingly
- Empower (create expectations) for employees, customers, and vendors with regard to ethics and fraud
- Understand fraud risks
- Monitor management:
    - Risk assessments
    - Antifraud policies and control (prevention and deterrence)
    - Assurance that controls are effective to ensure timely and accurate reporting (detection)
- Set the appropriate tone at the top
- Retain and compensate outside expertise when necessary
- Provide external auditors with evidence of the board of directors' commitment to and involvement in fraud risk management

PROTOCOL: A PLAN FOR REACTION TO ALLEGATIONS OF MISCONDUCT

One tool that can assist the board of directors is a written protocol that outlines its response when allegations of unethical behavior, fraud, and other corporate malfeasance come to light. Allegations and corporate reaction spin out of control because there is no planned approach to resolve the issues. A written protocol provides advance approval and authorization relative to the process and outlines who will be involved when suspicions of fraud or other allegations arise, no matter the source.

The response outlined in the protocol depends on the specificity and severity of allegations.[17]

PROTOCOL A

Assuming that the allegations are broad and general, such as a vague tip from an anonymous hotline, no real action can be taken other than reevaluating the highest likelihood where the alleged act could have happened and reconsidering any assessments of red flags. This assumes a strong antifraud environment and corporate culture, including fraud risk assessment, a hotline with properly trained personnel, and good fraud awareness training and programs.

The board of directors should ensure that at least two or three options for reporting wrongdoing have been created. The board needs to ensure that its response has been documented but, generally, no immediate action can be taken because the allegation lacks specificity. All discussions and reactions should remain confidential. Public companies may have the responsibility to inform their external auditor.

PROTOCOL B

Assuming that the allegations have some specificity (e.g., location), the board of directors knows where the activity may be occurring.

If the person making the allegation is unknown but enough information is provided to know where to begin looking (e.g., the department), the board must initiate action. Since the whistle-blower's allegations have not been substantiated with evidence, any investigative activities need to be confidential to the extent possible. Responsibility for investigating the initial allegations can be transferred from the board to the entity's general counsel, internal audit, and possibly the ethics/compliance committee.

Those charged with confidentially substantiating the allegations with some preliminary evidence need to use brainstorming techniques to consider approaches that may be useful to obtain further information and gain more specificity regarding the nature of the fraud or illegal act, the locations, the persons involved, and so on. The allegation may lead to the discovery of a variety of corporate malfeasance, such as bribery, kickbacks, financial statement frauds, asset misappropriation, or illegal acts.

PROTOCOL C

If the person making the allegation is known or there appears to be enough specificity to determine who is involved, the entity's general counsel, internal audit, or external professionals can be assigned to complete a preliminary investigation. The preliminary investigation may be facilitated through a scheduled audit or interviews for fact finding.

Given the specificity of the allegations and the ability to make further inquiries of the whistle-blower, brainstorming and other techniques can be used to develop an effective course of action to resolve the allegations. The protocol may require oral communication with the audit committee; the audit committee may then want to refine the investigative plan.

PROTOCOL D

Assuming specificity and allegations of severe misconduct, such as knowledge of the who, what, when, where, how, and why, especially by senior or executive management, the board may bring in special counsel. Further, for suspicions of severe misconduct of significant magnitude, the board will likely need qualified, experienced professionals to investigate the issues and to work with the board to ensure proper and timely resolution. Generally, any external fraud or forensic accounting professional should be independent of the entity's external auditor.

A fact-finding exercise must be undertaken to develop preliminary evidence to support the allegation. The objective is to preliminarily confirm the magnitude (severity) of the fraud and determine, based on evidence, and who is involved, including participants who may be external to the entity.

The board must develop a communication to the audit committee. The audit committee will determine how and when it will inform the external auditor. Once notified, the audit committee can contribute to and refine the investigative plan. The audit committee may hire its own legal counsel and investigators.

At some point, the entity has an obligation to communicate with shareholders, regulators, and others. The board of directors should work with legal counsel to determine appropriate timing in order to comply with applicable laws and regulations.

The protocols just described need to be fleshed out in detail. The office of risk management or outside consultant can be assigned the responsibility of developing the details. Getting into specifics of the protocol requires:

- An assessment of the entity's risk tolerance
- Knowledge of the adequacy of management's fraud risk assessment to identify exposures
- A listing of geographic locations, remembering that global operations increase risk
- Knowledge of industry business practices and industry fraud risks
- An understanding of the experience and sophistication of the board and audit committee with regard to fraud detection and investigation

A prerequisite for the development and execution of a protocol is a board and audit committee educated in fraud and fraud risk management and their involvement in the protocol activity.

To develop and execute the protocol, the board and audit committee must have a feel for a number of issues, such as:

- How good/reliable are the anonymous hotline and other sources of the allegations?
- What is the attitude of the employees, and how do they believe that the company would respond if an employee became a whistle-blower?
  - Do employees believe that the entity would take the allegations seriously?
  - How do whistle-blowers perceive that they will be treated?
- How effective are the antifraud entity-level controls?
- What do employee surveys concerning ethics, compliance, fraud, fraud awareness, and other similar topics reveal about the entity's culture?
- Is there more than one method to report fraud?
- Are there standardized reporting forms for allegations of fraud and other misconduct?
- How are anonymous calls made from outside the country handled? (Is the communication method modified for cross-country cultural concerns?)

- What is being done to address management override, collusion, violations of the foreign corrupt practices act, and other high-risk concerns?

If the protocol is detailed, thorough, and complete and has buy-in by the board and audit committee, the entity should be able to resolve allegations in an appropriate and timely manner.

The last thought:

> *In God We Trust. Everyone Else, We Examine.*
>
> —adapted from Michael Connelly's *Void Moon*

NOTES

1. BRT, *Statement on Corporate Governance* (September 1997): 4–5.
2. M. Kirdahy, ''Boards' Serve Management, Not Shareholders,'' *Forbes Magazine*, October 22, 2007; available at www.forbes.com/2007/10/22/sarbox-regulation-shareholders-lead-govern-cx_mk_1022boards.htm.
3. Pricewaterhouse Coopers (PWC). 2007. Global Best Practices: Building Blocks of Effective Corporate Boards (September). Available at www.globalbestpractices.com.
4. Office of Public Sector Information, *The Companies Act*, 2006; available at search.opsi.gov.uk/search?q=companies+act+2006+pdf&output=xml_no_dtd&client=opsisearch&proxystylesheet=opsisearch&site=default_collection.
5. E. H. Feroz, K. Park, and V. S. Pastena, ''The Financial and Market Effects of the SEC's Accounting and Auditing Enforcement Releases,'' *Journal of Accountancy Research* 29 (1991): 107–142. A. Shivdasani, ''Board Composition, Ownership Structure, and Hostile Takeovers,'' *Journal of Accountancy and Economics* 16 (1993): 167–198.
6. R. Johnson, R. Hoskisson, and M. Hitt, ''Board of Directors Involvement in Restructuring: The Effect Importance of Board Versus Managerial Controls and Characteristics,'' *Strategic Management Journal* 14 (1993): 33.
7. Sir A. Cadbury, *Financial Report of the Committee on the Financial Aspects of Corporate Governance* (London: Financial Reporting Council. London Stock Exchange, December 1992).
8. M. S. Beasley, ''An Empirical Investigation of the Relation between Board of Director Compensation and Financial Statement Fraud,'' Accounting Review (October 1996): 443–465. P. M. Dechow, R. G. Sloan, and A. P. Sweeney. ''Causes and Consequences of Earnings Manipulations: An Analysis of Firms Subject to Enforcement Actions by the SEC,'' *Contemporary Accounting Research* (Spring 1996): 1.
9. Gibson, Dunn & Crutcher LLP, ''New Companies Act of 2006: Impacts Upon Directors of U.K. Companies,'' December 7, 2006; available at www.gibsondunn.com/publications/Pages/NewCompaniesAct2006(CompaniesAct)ImpactsUponDirectorsofUKCompanies.aspx.
10. Ibid.

11. Pfizer, ''Pfizer Board of Directors to Initiate Investor Meeting,'' June 28, 2007; available at mediaroom.pfizer.com/portal/site/pfizer/?ndmViewId=news_view&newsId=20070628005559&newsLang=en.
12. J. Cai, J. L. Garner, and R. A. Walking, ''Electing Directors,'' Working paper, LeBow College of Business, Drexel University, November 10, 2008, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=1101924.
13. Ibid.
14. SEC, ''SEC Votes to Adopt Changes to Disclosure Requirements Concerning Executive Compensation and Related Matters,'' July 26 2006; available at www.sec.gov/news/press/2006/2006-123.htm.
15. F. Norris, ''Don't Like a Director? Spy on Him,'' *New York Times*, September 8 2006.
16. IIA, AICPA, and ACFE, ''Managing the Business Risk of Fraud: A Practical Guide'' (2008); available at www.acfe.com/documents/managing-business-risk.pdf.
17. These protocols were developed with the assistance of Steve Silver, West Virginia University Executive in Residence, 2007–2008.

Chapter 8

Audit Committees and Corporate Governance

INTRODUCTION

As discussed in prior chapters, financial reporting fraud is a relatively rare event. Unfortunately, all we hear in the media are those instances where some aspect of corporate governance has failed. We examine those failures as lessons learned: to learn what not to do as well as what to do. In the case of William Webster, the first chairman of the Public Company Accountability and Oversight Board (PCAOB), the aftermath was particularly damaging. Webster was considered one of America's most prestigious and influential citizens. However, because of the allegation that he failed to properly investigate the accounting problems at U.S. Technologies in his role as a chair of the company's audit committee, both the chairman of the Securities and Exchange Commission (SEC), Harvey Pitt, and Webster resigned under considerable fire. U.S. Technologies will be discussed in more detail later in the chapter.

For now, what is important to note is that an effective audit committee becomes integral to the antifraud environment by taking an active role in the prevention, deterrence, and detection of fraud. The audit committee facilitates this role by monitoring the effectiveness of the corporate ethics and compliance programs, monitoring management, and working with internal and external auditors to ensure that the entity has appropriate antifraud programs and controls in place to deter and identify fraud. Upon reasonable indicators of fraud, audit committees ensure that investigations are thorough and complete, working with external professionals when appropriate.

AUDIT COMMITTEE

The Sarbanes-Oxley Act (SOX) of 2002[1] and the SEC's related implementation rules[2] are intended to improve the quality of financial reports and necessitate that publicly traded companies revise and expand the functions, responsibilities, and charters of their audit committees Traditionally, many companies have formed audit committees as standing committees of outside directors to oversee the quality of the financial reporting process, internal control structure, and audit functions.

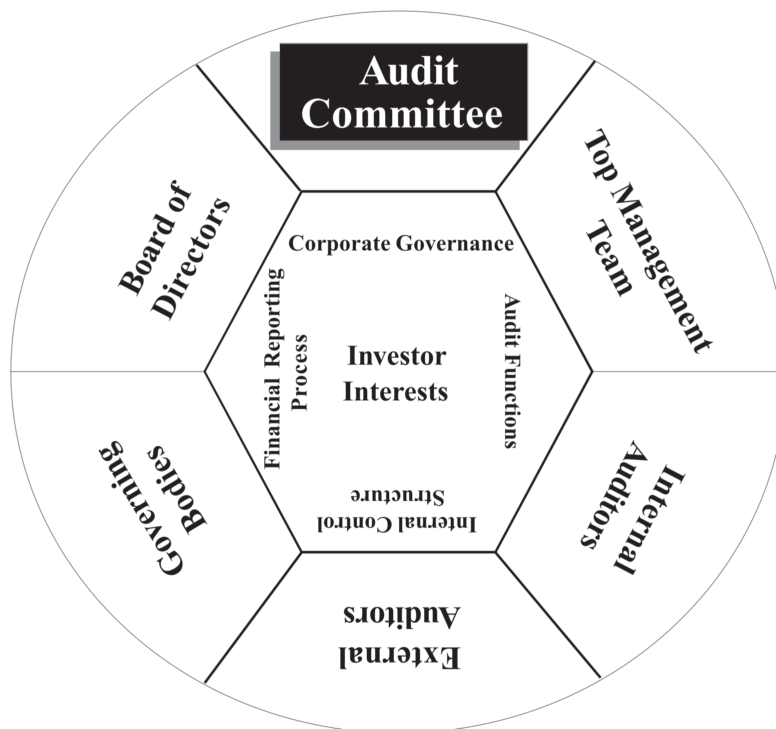


Exhibit 8.1 Audit Committee and Its Functions

Recently the new rules for audit committees set forth by the SEC, New York Stock Exchange (NYSE), and National Association of Securities Dealers (NASD) empower audit committees to function on behalf of the board by playing an important role in the corporate governance process to protect investors' interests and ensure corporate accountability. In this new capacity, the audit committee oversees the effectiveness of corporate government, the integrity of financial reports, the adequacy of the internal control structure, and the quality of the audit function, as depicted in Exhibit 8.1.

The success of audit committees in fulfilling their oversight responsibility depends on their working relationships with other members of corporate governance, including the board of directors, management, external auditors, internal auditors, and legal counsel, as well as regulatory and standard-setting bodies. Because the audit committee typically is created by a company's board of directors, its functions, responsibilities, and charters should be approved by the board. The audit committee must be independent of management in order to be able to discharge its monitoring responsibilities in overseeing the financial reporting process, internal control structure, and audit functions. Audit committees should establish a close working relationship with both internal and external auditors. Audit committees must have or obtain within a reasonable period the financial literacy necessary to understand applicable laws, regulations, and standards promulgated by regulatory

and standard-setting bodies as well as the ability to read and understand the four basic financial statements. The emerging interest in corporate governance, as evidenced by concerns from investor groups, regulators, and the public regarding financial statement fraud, underscores the importance of audit committees as a crucial element of corporate governance mechanisms. Former SEC chair Arthur Levitt rightfully stated, "Effective oversight of the financial reporting process depends to a very large extent on strong audit committees. Qualified, committed, independent, and tough-minded audit committees represent the most reliable guardians of the public interest."[3]

PCAOB's First Chair William Webster Steps Down

According to AccountingMalpractice.com, William Webster was one of the most prestigious and influential citizens in America. His pedigree includes being the director of the Central Intelligence Agency and the Federal Bureau of Investigation (FBI). He was a former federal judge who ascended to the CIA after successful coups against the New York mafia families while working as the director of the FBI under President Jimmy Carter. On October 25, 2002, he was named to head up the newly created PCAOB.

Just a few months prior to his PCAOB appointment, Webster resigned from the board of U.S. Technologies, where he was head of the board's audit committee. U.S. Technologies had been attempting to work its way through an (adverse) going-concern audit opinion. In February 2000, Webster accepted the position of audit committee chair of U.S. Technologies for compensation in the form of stock options (250,000 options at a price of $0.90 when the stock price was above $2.00 per share). In April 2001, he received another 400,000 options with an exercise price of $0.28 per share. In 2000, U.S. Technologies received a going-concern opinion based on material weaknesses in the financial and accounting structure, including a chief financial officer (CFO) lacking experience and deficiencies in recording material transactions and in the organization and retention of financial and accounting documents. BDO Seidman, an accounting firm, informed the company that the issues were more than economic; the records were inadequate to produce reliable financial statements and the audit firm had questions about management integrity and reliability. Webster and the audit committee dismissed BDO Seidman.

Because of allegations that Webster failed to properly investigate the accounting problems at U.S. Technologies and because SOX and the PCAOB were created to improve the accuracy and reliability of corporate disclosures, William Webster and then-SEC chairman Harvey Pitt came under considerable fire. Pitt resigned from the SEC and Webster stepped down about a week later.

By December 20, 2002, the SEC alleged that from June 1998 through August 2002, U.S. Technologies' chief executive officer (CEO), C. Gregory Earls, misappropriated approximately $13.8 million from investors. On April 23, 2004, in a related criminal proceeding, a jury convicted Earls of 22 counts of securities fraud, mail fraud, and wire fraud arising out of the same events and activities alleged in the SEC's complaint.

Source: United States v. C. Gregory Earls, No. 02-MAG-531 (S.D.N.Y.). See SEC Litigation Release No. 18031/March 12, 2003.

SOX and related SEC implementation rules significantly affect the structure, composition, functions, and responsibilities of audit committees. Underlying both SOX and the rules are the presumption that the presence of certain features in the audit committee is a prerequisite for the committee to effectively fulfill its oversight function. Specifically, the audit committee should be independent, competent, financially literate, adequately resourced, and properly compensated. SOX mandates these requirements for audit committees:

- The audit committee should be composed entirely of independent members of the board of directors.
- The audit committee should be directly responsible for the appointment, compensation, and oversight of the work of external auditors.
- The audit committee should have the authority to engage advisors.
- The audit committee should be properly funded to carry out its duties effectively.
- Auditors should report to the audit committee all "critical accounting policies and practices" used by the client.
- Public companies should disclose whether at least one member of their audit committee is a "financial expert."

The corporate governance principles of major stock exchanges (e.g., NYSE, NASDAQ, American Stock Exchange [AMEX]) also provide guidelines for audit committees, including the sole authority to hire, fire, and retain independent auditors to audit financial statements and to approve any permissible nonaudit services.

SOX and the SEC implementation rules have shifted some of management's financial reporting and audit involvements responsibilities to the audit committee. Exhibit 8.2 compares and contrasts the composition, attributes, structure, and functions of the audit committee as required by SOX and the SEC implementation rules with those of suggested best practices (benchmarks). The most noticeable differences are:

- SOX and SEC rules require a minimum of three independent members of the audit committees, whereas the benchmark suggests five independent members.
- SOX requires at least one member of the audit committee be designated as a "financial expert," while the benchmark suggests that all members of the audit committee should be financial experts.
- SOX requires rotation of the lead audit partner once every five years, whereas the benchmark suggests rotation of audit firm when there is a combination of circumstances that could impair the audit firm's independence from management.

The improvements in the audit committee enable the committee to effectively oversee internal controls, financial reports, and audit activities that result in reducing the likelihood of financial statement fraud.

Exhibit 8.2 Audit Committees

Provisions	Required by the Sarbanes-Oxley Act of 2002 and SEC Rules	Specific Best Practice Suggestions
I. Composition	1. The audit committee consists of at least three members. 2. Each member of the audit committee is independent as determined by the following two criteria: a. Members are barred from accepting any consulting, advisory, or other compensatory fee other than as a member of the board b. Members are not affiliated persons	1. The audit committee consists of five members. 2. All members of the audit committee are independent as defined by the applicable rules and regulations.
II. Functions	Audit committees: 1. Enhance the independence of audit functions 2. Hire, evaluate, and fire external auditors 3. Responsible for the appointment, compensation, retention, and oversight of the work of auditors 4. Approve all audit engagement fees and terms and significant nonaudit engagements of the independent auditor 5. Review of financial statements 6. Assessment of risks and vulnerabilities 7. Oversight of external and internal audits	Audit committees: 1. Approve all audit and nonaudit services 2. Hire, fire, and retain independent auditors 3. Review and approve budget for the internal audit function and have authority to hire and fire chief executive auditor 4. Assess risk management 5. Discuss annual and quarterly financial reports, including financial statements and management's discussion and analysis (MD&A) with management and independent auditors 6. Review the independent auditor's report on financial statements 7. Receive required information regarding auditor independence 8. Meet privately with external auditors 9. Meet privately with internal auditors 10. Review external auditors' audit plan, procedures, scope, and results 11. Review internal auditors' audit plan, procedures, scope, and results 12. Have unrestricted access to all company records 13. Review management strategic plans and business risk

(*continued*)

Exhibit 8.2 (*continued*)

Provisions	Required by the Sarbanes-Oxley Act of 2002 and SEC Rules	Specific Best Practice Suggestions
		14. Review corporate governance principles and monitors compliance with these principles 15. Review internal control structure disclosures and reporting controls and procedures 16. Review management report on ICFR 17. Review independent auditors' report on ICFR
III. Handling Complaints	Audit committees establish procedures for: 1. The receipt, retention, and treatment of complaints received by the company regarding accounting, internal controls, or auditing matters 2. The confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters	Audit committees establish procedures for the receipt, retention, and treatment of complaints received
IV. Advisors	The audit committee must have the authority to engage outside advisors, including counsel, as it determines necessary to carry out its duties.	The audit committee should retain professional outside advisors who are independent from management and internal and external auditors to assist the committee with various financial, audit, and corporate governance issues.
V. Funding	The audit committee must have appropriate funding for payment of compensation to any: 1. Registered public accounting firm engaged to render or issue an audit report or to perform other review or attest services 2. Advisor employed by the audit committee	Audit committees should be: 1. Adequately compensated in cash and stock 2. Legally protected from potential liabilities 3. Have sufficient funds to compensate external auditors for audit and nonaudit services and advisors for their legal and financial consulting
VI. Knowledge	1. All members of the audit committee should have knowledge and experience in financial reporting and auditing matters 2. At least one member of the committee is a financial expert who: a. Understands financial statements and accounting standards	1. All members of the audit committee must be financial experts 2. Each member of the audit committee should complete an orientation 3. Members of the audit committee should participate regularly in continuing education programs

	b. Has experience with application of accounting standards as related to accounting estimates, accruals, and reserves as well as preparing and auditing financial statements c. Has experience with internal accounting controls d. Understands audit committee functions	4. Members should retain outside advisors or educational consultants as they deem appropriate
VII. Certification	1. CEOs and CFOs certify the: a. Completeness and accuracy of financial statements b. Existence of disclosure controls and procedures c. Adequacy and effectiveness of internal controls 2. Management annual report on internal controls for financial reporting and assessment of those controls 3. Independent auditors attest to and report on the management's assessment of internal controls	1. Public companies should have an internal audit function either in-house or outsourced 2. Internal audit functions should have short-term and long-term audit plans addressing the company's risks and vulnerabilities 3. The audit committee should review and approve internal audit risk-based plans 4. The chief executive auditor (CEA) should have a direct line of communication and reporting responsibility to the audit committee 5. The CEA should meet with the audit committee in executive session 6. The CEA should attend all regularly scheduled audit committee meetings and report on internal auditors' findings 7. The audit committee should review and approve the CEO and CFO certification of financial statements, the management report on internal controls, and the independent auditors' report on management's assessment of internal controls 8. Continuous assessment of the internal controls structure should include an analysis of the overall risk environment and controls and information systems that address these risks
VIII. Auditor Rotation	The audit committee should: 1. Restrict the extent of nonaudit services provided by the auditor 2. Limit the employment by a company of audit firm personnel 3. Require five-year rotation of partners who have participated in the audit	1. The audit committee should consider rotating the accounting firms when: a. The firm has audited the company for a long period of time (e.g., over 15 years) b. One or more former partners, managers, or senior auditors of the firm are employed by the company

(*continued*)

Exhibit 8.2 (*continued*)

Provisions	Required by the Sarbanes-Oxley Act of 2002 and SEC Rules	Specific Best Practice Suggestions
	4. Direct the general accounting office to study the issue audit firm rotation	c. Significant nonaudit services are provided to the company 2. The audit committee should periodically (at least once every three years) evaluate auditors' independence from management
IX. Evaluation		Companies develop processes to evaluate, at least annually, the performance of their audit committee as a whole, the performance of each board committee, and the performance of each member of audit committee. This evaluation should compare the performance of the committee and its members to all applicable rules and regulations and stock exchange requirements in order to prevailing best practices for the audit committee.
X. Ethics Oversight		The audit committee is responsible for overseeing corporate ethics. 1. Development of corporate code of ethics, which defines ethical standards and skills required to: a. Foster ethical practice throughout the organization b. Verify adherence to applicable laws, rules, and regulations c. Verify compliance with appropriate accounting and auditing standards d. Establish proper whistle-blowing process to report possible ethical violations e. Endure fair resolution of conflicts of interest f. Prohibit business and financial misconduct including fraudulent activities 2. The audit committee should investigate and monitor periodically the compliance with the established code of ethics through the fair process that

	a. Ensures employees understand, apply, and adhere to the code of ethics b. Encourages employees to raise ethical issues and concerns as well as report possible ethical violations c. Conducts investigations of complaints, disciplines wrong-doers, and takes prompt corrective action d. Assesses employees' adherence to the established code of ethics and ethical performance of individual employees and the company as a whole
XI. Structure	The audit committee should: 1. Adopt the required written audit committee charter 2. Have a charter that describes structure, duties, responsibilities, functions, and composition of the committee 3. Evaluate its charter on an annual basis 4. Meet at least four times a year 5. Adopt corporate governance guidelines pertaining to the audit committee 6. Adopt a code of business conduct and ethics 7. Receive only directors' fees in cash or company stock options or other consideration ordinarily available to directors

AUDIT COMMITTEE ATTRIBUTES

The audit committee's function has evolved over the years. With recommendations of the Blue Ribbon Committee (BRC) and the new rules of the SEC and organized stock exchanges, it is viewed as an oversight function of corporate governance, the financial reporting process, the internal control structure, and audit functions. Yet until recently, there was no common view of audit committee attributes, no charter of what it should achieve, and no indication of whether to include the audit committee report in annual reports.

I. Audit Committee Composition

- Consists entirely of independent, outside directors (who have no material relationships with the company, its board of directors, and top executives, such as commercial, banking, accounting, industrial, characteristics, and familial relationships).
- All the members are financially literate (have a basic understanding of accounting, finance, and management issues).
- At least one member has financial expertise (accounting or related financial management education, knowledge, and experience).
- Consists of at least three members.

II. Audit Committee Structure

- Adopts the required written audit committee charter.
- Has a charter that describes structure, duties, responsibilities, functions, and composition of the committee.
- Evaluates its charter on an annual basis.
- Meets at least four times a year.
- Adopts corporate governance guidelines pertaining to the audit committee.
- Adopts a code of business conduct and ethics.
- Receives only directors' fees in cash, or company stock options, or other considerations ordinarily available to directors.

III. Audit Committee Resources

- Access to management and staff, as considered necessary.
- Competently staffed (e.g., accounting, legal).
- Adequately compensated (e.g., compensated in stock or cash).
- Legally protected from potential liabilities.
- Unrestricted access to company records and financial reports.
- Able to hire accounting, financial, and legal advisors.

IV. Audit Committee Authority

- Approves all nonaudit services.

- Hires, fires, and retains independent auditors.
- Retains legal, accounting, and other experts.
- Responsible for the appointment and compensation of auditors and oversight of their work.
- Establishes procedures for the receipt, retention, and treatment of complaints received.
- Reviews and approves budget for the internal audit function and has authority to hire and fire the chief internal auditor.
- Coordinates efforts of external and internal auditors.
- Has investigation powers.

V. Audit Committee Functions

- Promotes sound hiring policies for audit firm employees.
- Assesses risk management.
- Arranges meetings with management, internal auditors, and independent auditors.
- Discusses annual and quarterly financial reports, including financial statements and management's discussion and analysis with management and independent auditors.
- Reviews the independent auditors' report.
- Receives required information regarding auditor independence.
- Has private meetings with both external and internal auditors.
- External auditors have unrestricted access to the audit committee.
- Internal auditors have unrestricted access to the audit committee.
- Reviews external auditors' audit plan, procedures, scope, and results.
- Reviews internal auditors' audit plan, procedures, scope, and results.
- Has unrestricted access to all company records.
- Reviews management's strategic plans and business risk.
- Reviews corporate governance principles and monitors compliance with these principles.
- Reviews internal control structure disclosures and reports controls and procedures.
- Reviews management's assessment of the adequacy and effectiveness of internal controls.
- Reviews independent auditors' attestation on management's assessment of internal controls.
- Reviews management's certification of the accuracy, completeness, and fair presentation of financial statements in conformity with generally accepted accounting principles (GAAP).

AUDIT COMMITTEE ROLES AND RESPONSIBILITIES

The primary responsibilities of audit committees in the post-SOX era are to understand the implications of significant transactions regarding financial reporting and internal controls. Thus, the review of the effectiveness of internal controls and reliability of financial reports is an essential part of the audit committee's roles and responsibilities. The audit committee should review the adequacy and effectiveness of overall internal control relevant to operational, financial, and compliance controls, not just internal control over financial reporting (ICFR), and report publicly that it has undertaken the review. The audit committee should review:

- Management's assessment of the effectiveness of ICFR
- The independent auditor's report on the effectiveness of ICFR
- The independent auditor's report on the fair presentation of financial statements

INTERNAL CONTROLS

The audit committee should oversee the adequacy and effectiveness of the company's internal control structure to ensure:

- The efficiency and effectiveness of operations
- The reliability of financial reporting
- Compliance with applicable laws and regulations.

The committee's oversight of Section 404 on internal control is becoming more important as public companies are required to certify their ICFR. The audit committee should:

- Know the senior executive who is directly responsible and ultimately accountable for Section 404 compliance
- Understand the process of establishing and maintaining adequate and effective internal control
- Understand procedures for assessing the effectiveness of both the design and operation of ICFR
- Understand the proper documentation of compliance with Section 404
- Review management's report on the effectiveness of ICFR
- Review auditor reports expressing an opinion on management's assessment of the effectiveness of ICFR
- Evaluate the identified significant deficiencies and material weaknesses in internal control
- Be satisfied with management and auditor efforts as well as reports on ICFR

- Ensure that management has properly addressed the identified material weaknesses

The audit committee is responsible for assessing management's internal control activities and issues. Sixteen pertinent questions that committee members should ask include:

1. What are the internal control priorities?
2. Are there adequate internal control investments?
3. Are internal control resources properly allocated?
4. Is the company getting the right return for its investment in internal control?
5. Are entity-level controls adequate and effective?
6. Are process-level controls adequate and effective?
7. Have management and the independent auditor coordinated their plans to implement the requirements of the SEC's Interpretive Guidance and PCAOB's Auditing Standard No. 5?
8. Are the design and operation of ICFR effective?
9. Are the design and operation of internal control over operational performance (ICOP) effective?
10. Are the design and operation of internal control over compliance functions (ICCF) effective?
11. Is the management report on ICFR appropriate?
12. Is the independent auditor's report on ICFR appropriate?
13. What are the causes and effects of reported material weaknesses in ICFR?
14. What, if any, remediating actions have been taken or are planned by management to correct reported material weaknesses?
15. Has the independent auditor issued a report on management's corrections of the reported material weaknesses?
16. What are the effects of the internal control's significant deficiencies and material weaknesses on potential misstatements in financial statements?

FINANCIAL REPORTING

The audit committee should oversee the financial reporting process by reviewing annual and quarterly financial statements, including the following:

- Management discussion and analysis
- Accounting principles, practices, estimates, and reserves
- Independent auditors' suggestions, comments, and adjusting and classification entries

The committee is responsible for overseeing the integrity, reliability, quality, and transparency of the company's financial disclosures. In the post-SOX period, the audit committee should prepare and submit a formal annual report to the shareholders stating that:

- Financial statements included in the annual report on Form 10-K or Form 10-KSB are prepared in accordance with GAAP.
- The committee has adopted a charter and has satisfied its oversight responsibilities as specified in the proxy statement.
- The committee has reviewed the audited financial statements with management.
- The committee has discussed with the independent auditor those matters required to be communicated to the committee in accordance with generally accepted auditing standards (GAAS).
- The committee has received the independent disclosures from the independent auditor and has discussed the matters relevant to auditor independence.
- The committee has discussed with management and the independent auditor their reports on ICFR.

AUDIT ACTIVITIES

The audit committee is responsible for overseeing both internal and external audit activities. The committee has direct responsibility for hiring, compensating, and firing the company's independent auditor and chief audit executive (CAE; the head of the internal audit department). Sections 201 and 202 of SOX require the company's audit committee to preapprove all audit and permissible nonaudit services. The preapproval of permissible nonaudit services may be delegated to a member of the audit committee who must present preapproved nonaudit services to the full committee in its regular meeting. Thus, the audit committee must establish preapproval policies and procedures to:

- Increase the committee's knowledge and understanding of all permissible nonaudit services
- Evaluate the qualifications of providers of preapproved nonaudit services
- Select the best provider, considering the necessary reinforcement of auditor independence from management

Although SOX and SEC-related implementation rules permit certain tax services to be performed by the company's independent auditor contemporaneously with audit services, the PCAOB in its Ethics and Independence Rule 3523 limits the performance of a number of tax services, such as tax shelters. Both the independent auditor and the CAE should be held ultimately accountable to the audit committee.

The audit committee should receive and review reports of the independent auditors on financial statements and ICFR. The committee should also receive and review significant internal audit reports. On July 24, 2007, the PCAOB proposed its new Ethics and Independence Rule 3526 concerning communications with audit committees and an amendment to its existing tax services rule along with an implementation schedule for the tax services rule.[4] The proposed Rule 3526 would require independent auditors to communicate to the company's audit committee any relationships between the audit firms and the company that may reasonably be thought to bear on the auditor's independence. This communication would be required both before the auditor accepts a new engagement and annually for continuing engagements.

HealthSouth: Former CEO Scrushy Aquitted

In 2004, HealthSouth disclosed that a forensic audit by PricewaterhouseCoopers found fraudulent activities totaling between $3.8 billion and $4.6 billion. Bryan P. Marsal, the company's chief restructuring officer, said the fraud included:

- $2.5 billion in fraudulent accounting entries from 1996 to 2002
- $500 million in incorrect accounting for goodwill and other items involved in acquisitions from 1994 to 1999
- $800 million to $1.6 billion in ''aggressive accounting'' from 1992 to March 2003

Shareholders and bondholders sued the company and its previous auditors and investment bankers. HealthSouth is one of the nation's largest health care services providers with a chain of rehabilitation facilities across the country. The company boasts a vast network of highly skilled physicians and clinicians, providing access to high-quality health care, including inpatient rehabilitation, outpatient rehabilitation, long-term acute care hospitals, home health, and rehabilitation technology.

Despite what prosecutors described as ''persuasive evidence,'' the federal government's string of victories in corporate corruption cases ended in 2005 when former CEO and chairman of HealthSouth, Richard M. Scrushy, was acquitted on 36 counts related to the accounting fraud. The verdict came in spite of the testimony of more than six former Scrushy lieutenants who outlined his role in the fraud. Further, 15 executives, including five CFOs, had previously pleaded guilty or been convicted of participating in the fraud. A former CFO, William T. Owens, even presented a secretly recorded conversation with Scrushy, who discussed the illegal activity. Scrushy's defense team appeared to be successful at undermining the credibility of some of the witnesses and exploiting the complexity of the case, which is reflected in the length of the trial: five months of testimony. Perhaps more important to Scrushy's success was what Alabama radio host Paul Finebaum described as playing the ''race card'' and playing the ''religion card.'' Mr. Scrushy had attended a predominantly white church in an affluent suburb of Birmingham, Alabama. After his legal troubles began, Scrushy joined a predominantly black church and preached at several black churches around the city. Several pastors and congregants from black churches appeared each day in court with him, and several jurists indicated they would buy stock in a company led by Scrushy.

In a bizarre turn, Richard Scrushy was eventually convicted and sentenced to 6 years and 10 months in prison. However, the conviction was not directly related to the HealthSouth

accounting fraud. In this second trial, Scrushy was accused by prosecutors of paying Alabama governor Don Siegelman $500,000 for a seat on the hospital regulatory board. Scrushy was convicted of bribery, conspiracy, and four counts of mail fraud, while former governor Siegelman was sentenced to 7 years and 10 months after his conviction on similar charges.

Sources: Milt Freudenheim, ‘‘Audit Finds as Much as $4.6Billion in Fraud,’’ *New York Times*, January 21, 2004. HealthSouth, ‘‘What We Do,’’ available at www.healthsouth.com/what_we_do/default.asp. Simon Romero and Kyle Whitmire, ‘‘Former Chief of HealthSouth Acquitted in $2.7 Billion Fraud,’’ *New York Times*, June 29, 2005. Laurence Viele Davidson, ‘‘Scrushy, Ex-Governor Convicted,’’ *Philadelphia Inquirer*, June 20, 2006. Laurence Viele Davidson, ‘‘HealthSouth’s Scrushy Gets 6 Years in Prison,’’ *Washington Post*, June 29, 2007.

AUDIT COMMITTEE CHARTERS

The audit committee charter should be prepared and approved by the board of directors, periodically reviewed and modified as necessary, and disclosed at least triannually in the annual report to shareholders or in a proxy statement. A carefully developed charter is the cornerstone for ensuring the proper structure, composition, and qualifications of the audit committee. The primary purpose of formally adopting a charter is to establish the audit committee as a functional element of the company’s corporate governance. Thus, the audit committee charter will be viewed as a compliance document designed to be an effective mechanism of corporate governance.

The SEC advocates that the audit committee charter contain sufficient details and accountability to discourage financial statement fraud resulting from earnings management and accounting abuses that reduce the quality and integrity of financial reports. The new rules also require that audit committees recommend, based on discussions with management and external auditors, to the board of directors that the financial statements be included in the company’s annual report and that the committee believes that financial statements are fairly presented, in all material respects, in conformity with GAAP. There is tremendous support for this improved oversight responsibility of audit committees; however, now it is more likely that audit committee members will be personally named in litigation for potential negligence regarding alleged financial statement fraud. The SEC argues that existing safe harbors in new rules will protect audit committee members from litigation risk and potential liability under federal and state laws; nevertheless, carelessly drafted audit committee charters could provide sophisticated lawyers with an unintended road map of duties to which audit committee members may be held accountable and liable.

To prevent unwanted increased liability for audit committee members under the new rules, companies must seek the advice of legal counsel, including securities litigation specialists, to identify potential weaknesses in the charter that could be exposed in litigation. When establishing or redesigning their charters in conformity with the

requirements of the new rules on audit committees, publicly traded companies are strongly advised to consult with experts in corporate governance and audit committees to properly protect audit committee members and the company. The improved effectiveness of the audit committees under the new rules is expected to decrease the likelihood of financial statement fraud by providing the committees with the tools to prevent and detect fraudulent financial activities. Publicly traded companies should establish their charters according to their business environment and specifications, their audit committees' attributes, and the requirements of the new rules. Exhibit 8.3 presents a sample of a charter being suggested by one of the Big Five professional service firms.

CHAIRPERSON OF AUDIT COMMITTEES

The audit committee chair can play an important role in setting a tone and standard for other members to improve their effectiveness. The chair of the audit committee should establish a cooperative working relationship with the following:

- Board of directors
- Top management team, including the CEO and CFO
- Director of the internal audit function
- Lead audit partner

The chair can achieve such a relationship by having regular private meetings with the listed parties.

The new rules have expanded responsibilities and functions, practices, and the frequency and timing of the committee meetings with other constituencies of corporate governance. It is perhaps more practical for the chair of the audit committee to discuss the committee oversight functions with the top management team as well as with internal and external auditors before the full committee meets with these groups. Such a meeting would help to assess the necessary areas of oversight and to establish a definitive timeline for the entire year, including activities pertaining to the internal financial reporting process under the new rules.

AUDIT COMMITTEE REPORT

The BRC recommended and the SEC requires that an audit committee report be disclosed annually in the proxy statement. The audit committee must specify in this report whether the committee has:

- Reviewed and discussed the audited financial statements with management
- Discussed with the external auditors those matters required to be communicated to the audit committee in accordance with GAAS

Exhibit 8.3 Sample Audit Committee Charter

The following is a sample Audit Committee Charter designed to assist boards and their Audit Committees in their consideration of the new rules adopted by the SEC, NYSE, NASDAQ, and AMEX. This sample should be customized to each company's needs. Boards and their audit committees should consult corporate counsel prior to the adoption of an audit committee charter because this sample charter does not render or substitute for legal advice.

Audit Committee Charter

This Audit Committee Charter (Charter) has been adopted by the Board of Directors (the Board) of [name of company] (the Company). The Audit Committee of the Board (the Committee) shall review and reassess this charter annually and recommend any proposed changes to the Board for approval.

Role and Independence: Organization

The Committee assists the Board in fulfilling its responsibility for oversight of the quality and integrity of the accounting, auditing, internal control, and financial reporting practices of the Company. It may also have such other duties as may from time to time be assigned to it by the Board (See "*Additional Functions Frequently Assigned to Audit Committees*." Depending on the circumstances, it may be appropriate to incorporate some of these additional roles and duties in the charter.) The membership of the Committee shall consist of at least three directors who are each free of any relationship that, in the opinion of the Board, may interfere with such member's individual exercise of independent judgment. Each Committee member shall also meet the independence and financial literacy requirements for serving on audit committees, and at least one member shall have accounting or related financial management expertise, all as set forth in the applicable rules of the [select as appropriate: New York Stock Exchange/NASDAQ/American Stock Exchange]. The Committee shall maintain free and open communication with the independent auditors, the internal auditors, and Company management. In discharging its oversight role, the Committee is empowered to investigate any matter relating to the Company's accounting, auditing, internal control, or financial reporting practices brought to its attention, with full access to all Company books, records, facilities, and personnel. The Committee may retain outside counsel, auditors, or other advisors.

One member of the Committee shall be appointed as chair. The chair shall be responsible for leadership of the Committee, including scheduling and presiding over meetings, preparing agendas, and making regular reports to the Board. The chair will also maintain regular liaison with the CEO, CFO, the lead independent audit partner, and the director of internal audit.

The Committee shall meet at least four times a year, or more frequently as the Committee considers necessary. At least once each year the Committee shall have separate private meetings with the independent auditors, management, and the internal auditors.

Responsibilities

Although the Committee may wish to consider other duties from time to time, the general recurring activities of the Committee in carrying out its oversight role are described as follows. The Committee shall be responsible for:

- Recommending to the Board the independent auditors to be retained (or nominated for shareholder approval) to audit the financial statements of the Company. Such auditors are ultimately accountable to the Board and the Committee, as representatives of the shareholders.

- Evaluating, together with the Board and management, the performance of the independent auditors and, where appropriate, replacing such auditors.
- Obtaining annually from the independent auditors a formal written statement describing all relationships between the auditors and the Company, consistent with Independence Standards Board Standard Number 1. The Committee shall actively engage in a dialogue with the independent auditors with respect to any relationships that may impact the objectivity and independence of the auditors and shall take, or recommend that the Board take, appropriate actions to oversee and satisfy itself as to the auditors' independence.
- Reviewing the audited financial statements and discussing them with management and the independent auditors. These discussions shall include the matters required to be discussed under Statement of Auditing Standards No. 61 and consideration of the quality of the Company's accounting principles as applied in its financial reporting, including a review of particularly sensitive accounting estimates, reserves and accruals, judgmental areas, audit adjustments (whether or not recorded), and other such inquiries as the Committee or the independent auditors shall deem appropriate. Based on such review, the Committee shall make its recommendation to the Board as to the inclusion of the Company's audited financial statements in the Company's Annual Report on Form 10-K (or 10-KSB [or the Annual Report to Shareholders, if distributed before the filing of the Form 10-K]).
- Annually issuing a report to be included in the Company's proxy statement as required by the rules of the Securities and Exchange Commission.
- Overseeing the relationship with the independent auditors, including discussing with the auditors the nature and rigor of the audit process, receiving and reviewing audit reports, and providing the auditors full access to the Committee (and the Board) to report on any and all appropriate matters.
- Discussing with a representative of management and the independent auditors: (1) the interim financial information contained in the Company's Quarterly Report on Form 10-Q (or 10-QSB) before its filing, (2) the earnings announcement before its release (if practicable), and (3) the results of the review of such information by the independent auditors. (These discussions may be held with the Committee as a whole, with the Committee chair in person, or by telephone.)
- Overseeing internal audit activities, including discussing with management and the internal auditors the internal audit function's organization, objectivity, responsibilities, plans, results, budget, and staffing.
- Discussing with management, the internal auditors, and the independent auditors the quality and adequacy of and compliance with the Company's internal controls.
- Discussing with management and/or the Company's general counsel any legal matters (including the status of pending litigation) that may have a material impact on the Company's financial statements and any material reports or inquiries from regulatory or governmental agencies.

The Committee's job is one of oversight. Management is responsible for preparing the Company's financial statements and the independent auditors are responsible for auditing those financial statements. The Committee and the Board recognize that management (including the internal audit staff) and the independent auditors have more resources and time and more detailed knowledge and information regarding the Company's accounting, auditing, internal control, and financial reporting practices than the Committee does; accordingly, the Committee's oversight role does not provide any expert or special assurance as to the financial statements and other financial information provided by the Company to its shareholders and others.

- Received from the external auditors a letter revealing matters that, in the auditors' judgment, may reasonably be thought to bear on the auditors' independence from the company and discussed with them their independence
- Recommended to the board of directors that the company's audited financial statements be included in the annual report on Form 10-K or Form 10-KSB based on discussions with management and external auditors

SOX- and SEC-related implementation rules require publicly traded companies to include a report of the audit committee in their proxy statement annually and to publish the audit committee charter in their proxy statement at least once every three years. The current mandatory audit committee disclosures are the following:

- Annual report on the audit committee
- Reporting of the audit committee charter in the proxy statement at least once every three years
- Disclosure in the proxy statement of whether the committee had fulfilled its responsibilities as specified in the charter

These enhanced mandatory audit committee disclosures are expected to encourage more vigilant audit committee oversight function, improve corporate governance, foster the public's confidence in the financial reporting process, and promote audit efficacy.

The audit committee report should indicate that the audit committee has done the following:

- Reviewed and discussed with management the company's audited financial statements
- Discussed their findings and other matters regarding audited financial statements with the independent auditors
- Received and reviewed the written disclosures from auditors regarding their independence
- Recommended to the board of directors that the audited financial statements be included in the company's annual report on Form 10-K or 10-KSB based on discussions with management and external auditors

Publicly traded companies listed on organized stock exchanges (NYSE, AMEX, NASDAQ) are required to include the audit committee charter in their proxy statement at least once every three years.[5] The audit committee charter states the committee's responsibilities, size, composition, authority, meetings, diligence, financial literacy, and independence.

The usefulness of this mandatory reporting has been challenged. Critics argue that such a mandatory reporting requirement will increase audit committee's liability,

which will eventually result in either higher compensation for audit committee members or fewer qualified directors willing to serve on audit committees. Furthermore, the financial reporting oversight function of the audit committee has its limits because (1) management is primarily responsible for the fair presentation of financial statements, which conform to GAAP, (2) auditors are responsible for providing reasonable assurance regarding the fair presentation of financial statements in conformity with GAAP, and (3) the audit committee is not adequately resourced and staffed to shoulder the onerous legal responsibility of ensuring the reliability of financial statements.

Proponents (the BRC, SEC, NYSE, NASD) of mandatory audit committee reporting argue that such reports will improve integrity, quality, reliability, and transparency of financial reports because the reports will indicate that financial statements are useful and reliable, the audit was thorough, and the auditors have no flagrant conflicts of interest. This should reduce the information risks that may be associated with published audited financial statements.

AUDIT COMMITTEE ROLES IN PREVENTING AND DETECTING FINANCIAL STATEMENT FRAUD

The Treadway Commission recognized that audit committees play an important role in preventing and detecting financial statements fraud. The new guidance on audit committees by SOX, SEC, NYSE, AMEX, and NASDAQ has improved the effectiveness of audit committee oversight functions pertaining to corporate governance, the financial reporting process, the internal control structure, and audit functions, as depicted in Exhibit 8.1. These improved and expanded audit committee functions and practices enhance the integrity and quality of financial reports and contribute to preventing and detecting financial statement fraud. Toby S. F. Bishop, director of Deloitte's Forensic Center, has suggested these 10 fraud prevention and detection tips for audit committees:

1. Evaluate management's assessment of the significance and likelihood of your company's fraud risks, especially the pressure to meet earnings expectations.
2. Evaluate the internal control best practices that management has implemented to address each fraud risk.
3. Evaluate the internal auditors' testing of the effectiveness of each fraud control.
4. Ensure that your company periodically uses a research-based tool to measure the effectiveness of the CEO's efforts to create the right tone at the top to promote ethical behavior and deter wrongdoing.
5. Tell management you have zero tolerance for any cooking the books. Continuously evaluate management's integrity. Even small untruths are telling.
6. Ensure that your internal auditors report directly and candidly to you and have sufficient resources to do a world-class job.

7. Ensure that your internal auditors continually conduct financial statement and other fraud detection tests using the latest computer-assisted methods.
8. Where possible, have your quarterly financial statements tested before release, using the latest financial statement fraud detection tools.
9. For large companies, attach a ''fraud sentinel'' to your computer system to detect potentially fraudulent transactions on a real-time basis.
10. Have your independent auditors and fraud specialists critically evaluate the results of these items.[6]

ANTIFRAUD APPLICATIONS FOR PRACTICE

According to ''Managing the Business Risk of Fraud: A Practical Guide,''[7] these are roles, responsibilities, and characteristics of good audit committees:

- The audit committee should be independent in perception and in fact.
- The committee should have membership that includes at least one financial expert.
- The audit committee needs to meet frequently and long enough to fulfill their responsibilities.
- The committee needs to prepare sufficiently in advance of board and audit committee meetings.
- The audit committee needs to play an active oversight role in management's fraud risk assessment.
- The committee members need to discuss with the external auditor their plans with respect to fraud detection.
- Perhaps most important, the audit committee needs to recognize and address the fact that the major frauds result from management's collusion and override of controls, the Achilles' heel of the control system.

AUDIT COMMITTEE MEETINGS

Best practices with regard to audit committee meetings suggest that while executive management may be included in portions of the meeting, other portions should be conducted separately from executive management. The focus of the meetings with executive management should include a discussion and evaluation of management plans to deter, prevent, and detect fraudulent behavior.

Those portions of the meetings where executive management is excluded should include interactions with knowledgeable employees, financial managers, internal auditors, and the external auditors. Discussions with each of these professionals should include candid dialog while encouraging openness, honesty, and trust. The external auditors should be questioned about their procedures and audit practices

designed to detect fraud, including management override and collusive frauds. In all of these meetings, the audit committee needs to ask the tough questions.

In meetings with executive management, audit committee members should ask the following:

- Are you aware of any allegations of fraud?
- Have you been involved in or committed any fraudulent acts or activities that violate laws, regulations, or company policy and procedures?
- Have you acted in any manner that makes you feel uncomfortable?
- Who might have the best opportunity to commit fraud in this organization?
- Is there a reason why you or another employee might commit fraudulent or unethical behavior?
- What do you think should happen to persons who commit unethical or fraudulent acts?
- What is your level of job satisfaction:
  - Do you enjoy leading this organization?
  - Do you feel that you are treated fairly?
  - Are you experiencing any problems or concerns, personally or with regard to company issues?

In meetings with knowledgeable employees (including those from outside of accounting and finance) and financial managers, the audit committee should ask the following:

- Are you aware of any allegations of fraud?
- Have you been involved in or committed any fraudulent acts or activities that violate laws, regulations, or company policy and procedures?
- Have you been asked to act in any manner that makes you feel uncomfortable?
- Who might have the best opportunity to commit fraud in this organization?
- Is there a reason why you or a coworker might commit fraudulent or unethical behavior?
- What do you think should happen to persons who commit unethical or fraudulent acts?
- What is your level of job satisfaction:
  - Do you enjoy working here?
  - Do you feel that you are treated fairly?
  - Are you experiencing any problems or concerns, personally or with regard to company issues?
  - Is there anything that we might do for you?

In meetings with internal and external auditors, the audit committee questions may include:[8]

- Are you aware of any allegations of fraud?
- Have you discovered or identified any violations of laws, regulations, GAAP, or company's policies and procedures?
- Have you been asked to act in any manner that makes you feel uncomfortable?
- Who might have the best opportunity to commit fraud in this organization?
- Are you comfortable with the significant accounting policies selected by management and their application to this company's specific facts and circumstances, including consistency, clarity, and completeness?
  - First-time applications of accounting policies and procedures?
  - Significant unusual transactions?
  - Controversial or emerging areas where guidance may be lacking?
- Are you comfortable with management's qualitative and quantitative judgments and assumptions with regard to significant and sensitive accounting estimates?
- What significant audit adjustments have you identified?
  - Were those identified adjustments recorded?
  - Why didn't management's system of internal controls identify (detect) those issues?
- What disagreements with management arose during your work, and how were those issues resolved?
- What problems did you encounter during the audit with regard to your interactions with executive management, including:
  - Unreasonable delays in beginning the audit work?
  - Unreasonable delays in obtaining needed information and supporting documentation?
  - An unreasonable timetable for completion?
  - Unavailability of personnel:
    - Accounting and financial personnel?
    - Nonaccounting personnel?
- Did you discover any illegal acts? If so what was the act, the circumstances of the act, and the effect of the act on the financial statements?

ADDRESSING CONCERNS OF MANAGEMENT OVERRIDE AND COLLUSION

The audit committee needs to approach the issue of management override and collusion proactively.[9] While management has responsibility for the fraud risk assessment

process and antifraud environment, with respect to management override and collusive fraud that involves top management, it hardly makes sense for management to be asked to police itself.

Another reason why the audit committee should consider a proactive approach to management override and collusion is because of the circularity that can arise with the external auditor who is assessing and addressing the risk. If audit committee members rely on the external auditor to assist them in their oversight role relative to evaluating management's fraud risk assessment process, have the committee members considered that the external auditor may be relying, to some extent, on the audit committee's own processes for the same or similar purposes? Audit committees need to recognize the potential circularity of this type of reliance: The auditor relies on the audit committee to assess and address the risk of collusive frauds and management override, and the audit committee is relying on the auditor to fulfill that oversight role.

A couple of other thoughts: While a good antifraud tool such as a hotline usually is effective, audit committees need to understand that such an approach is reactive, not approach. When collusive and override fraud occurs, the system of controls has been violated. In such cases, management override and collusive frauds cannot be prevented, only detected.

To be proactive, the audit committee should consider ensuring the following:

- Audit committee members have knowledge, education, awareness, and sophistication regarding the various fraudulent management override and collusive schemes that may be perpetrated by management.
- The internal audit group has knowledge, education, awareness, and sophistication concerning the various fraudulent management override and collusive schemes that may be perpetrated by management.
- The external auditor has knowledge, education, awareness, and sophistication concerning the various fraudulent management override and collusive schemes that may be perpetrated by management.
- The audit committee has reviewed the comprehensive fraud risk assessment provided by management but also considers how collusive fraud and management override schemes are mitigated and detected.
- The audit committee periodically participates in continuing education programs that can prepare members for appraising management's fraud risk assessment.
- Audit committee members identify who has the specific responsibility for the collusive and management override fraud risk assessment process: themselves, internal audit, or the independent audit group.
- The audit committee interacts with personnel beyond executive management and asks tough questions of knowledgeable employees, financial managers, internal auditors, and the external auditors.

ACTING ON ALLEGATIONS OF UNETHICAL AND FRAUDULENT CONDUCT

Once allegations of unethical behavior or fraudulent acts have been made, the audit committee must consider, develop, and evaluate at least some preliminary corroborative evidence. Assuming the allegations appear warranted, the audit committee should seek the advice of legal counsel and have a "reaction protocol" in place that identifies those conditions that spark additional work in order to discern the answers to the salient questions: who, what, when, where, and how, in addition to the protocol being followed. Assuming that allegations of fraud have preliminary substantiation, tough questions for company leadership, including individuals from executive management, knowledgeable employees, and financial managers, must include:[10]

- Who do you think did this?
- Who could you vouch for?
- Did you do this/any other fraud act?
- Did you ever take . . . ?
- Have you ever participated in . . . ?
- Have you ever violated company policy?
- Do you think an act (e.g., vendor billing scheme) really occurred? What do you think is the cause of the missing . . . ?
- Who would have the best opportunity?
- Is there a reason why you or a coworker might do . . . ?
- What do you think should happen to the person who did this?
- Have you ever borrowed money/merchandise?
- Have you ever considered doing this?
- What would be the easiest way to accomplish . . . ?
- How do you feel about this audit, investigation (e.g., It is a witch hunt!)?
- When this investigation is complete, how will you feel personally?
- Under what circumstances might this . . . be okay?
- Do you think the company is to blame for this?
- If you did this, what would you be worried about?
- What is your level of job satisfaction:
  - Do you like working here?
  - Do you feel that you are treated fairly?
  - Any problems?
  - Anything that I can do for you?

The last thought:

He who asks is a fool for five minutes, but he who does not ask remains a fool forever.

—Chinese proverb

NOTES

1. See www.sec.gov/about/laws/soa2002.pdf.
2. SEC Releases Nos. 33-8220 and 34-47654, *Standards Relating to Listed Companies Audit Committees* (Washington, DC: U.S. Government Printing Office, 2003).
3. Levitt's statement of February 8, 1999, is available at www.sec.gov.
4. PCAOB, ''Board Proposes New Ethics and Independence Rule Concerning Communications with Audit Committees and an Amendment to Its Existing Tax Services Rule and Adjusts Implementation Schedule for Tax Services Rule,'' July 24, 2007; available at www.pcaob.org/News_and_Events/News/2007/07-24.aspx.
5. SEC requires exchange listing standards for Audit Committees. 2003; available at www.sec.gov/news/press/2003-43.htm.
6. Bishop, Toby, ''Ten Tips for Preventing Corporate Fraud.'' VisionQwest Resource Group, Inc., 2009; available at www.vqrginc.com/fraud.html.
7. IIA, ACFE, and AICPA, ''Managing the Business Risk of Fraud: A Practical Guide'' (2008); available at www.aicpa.org/download/audcommctr/Managing_the_Business_Risk_of_Fraud.pdf.
8. Adapted from the AICPA Audit Committee Toolkit, ''Discussions to Expect from the Independent Auditor''; available at www.aicpa.org/audcommctr/toolkitsgovt/Discussions_With_Independent_Auditor.htm.
9. Scott Fleming, Steve Silver, and Richard Riley, ''Collusive Management Fraud: The Audit Committee's Oversight Role,'' *CPA Journal October* (2008); available at findarticles.com/p/articles/mi_qa5346/is_200810/ai_n30993408.
10. Protocols were discussed in Chapter 7. Questions in this area were adapted from David Zulawski and Douglas Wicklander, *Practical Aspects of Interview and Interrogation*, 2nd ed. (Boca Raton, FL: CRC Press, 2002).

Chapter 9

Management Responsibility

INTRODUCTION

Management plays an important role in ensuring responsible and effective corporate governance by managing the business of the corporation to create shareholder value. Management, through its delegated authority from the board of directors, is responsible for establishing and executing the corporate strategies, managing effective and efficient utilization of resources, directing and coordinating operational activities, and safeguarding assets. To fulfill its responsibilities, management should design and implement sound accounting systems that provide reliable and high-quality financial reports, establish and maintain an effective internal control system, and comply with applicable laws and regulations. Post–Sarbanes-Oxley Act (SOX), management is responsible for certifying the effectiveness of internal control over financial reporting (ICFR), in addition to the accuracy and completeness of financial reports. Management is an important member of corporate governance.

Consider Adelphia, a failure of managerial leadership and a related-party nightmare. Founded in 1952 by John Rigas, Adelphia, a cable television company, provided diversification against declining revenues in Rigas's movie theaters. The company went public in 1986, yet the Rigas family retained control over Adelphia through its ownership structure. By 2000, Adelphia was the sixth largest cable television and telecommunications service provider in the United States. In 2002, investors discovered that Adelphia backed $2.3 billion worth of personal loans to the Rigas family; in addition, other concerns about operational performance and misleading company disclosures came to light. Adelphia's stock price declined from about $30 per share in January 2002 to $0.30 per share in June 2002, and the stock was delisted from the NASDAQ market. Adelphia filed for bankruptcy under Chapter 11 in June 2002.[1]

MANAGEMENT FINANCIAL REPORTING RESPONSIBILITIES

Management is primarily responsible for the quality, integrity, and reliability of the financial reporting process, as well as the fair presentation of financial statements in conformity with generally accepted accounting principles (GAAP). Management

is also accountable to users of financial statements, particularly investors and creditors, in ensuring that published financial statements are not misleading and are free of material errors, irregularities, and fraud. To effectively discharge its financial reporting responsibility, management should do the following:

- Identify and assess the circumstances, conditions, and factors that can lead to financial statement fraud
- Assess and manage the risk of financial statement fraud associated with the identified circumstances, conditions, and factors
- Design and implement an adequate and effective internal control process for prevention and detection of financial statement fraud

Management is primarily responsible for the reliability of the company's financial reports and ICFR. In the post-SOX period, management is responsible for the following:

- Designing and implementing appropriate disclosure controls and procedures to ensure that reliable financial information is being disclosed
- Designing and maintaining adequate and effective ICFR to ensure reliability of financial reports and fair presentation of financial statements in conformity with GAAP
- Evaluating the effectiveness of the company's disclosure controls and procedures and disclosing its conclusions as of the end of the reporting period
- Evaluating the effectiveness of ICFR as of the end of the reporting period and disclosing significant internal control deficiencies to the company's audit committee and independent auditor and disclosing material weaknesses to shareholders
- Designing and maintaining an appropriate accounting system to ensure production of accurate and complete financial information
- Preparing and certifying financial statements that reflect fair presentation of the financial position and results of operation in conformity with GAAP

Management is primarily responsible for the fair and true presentation of financial statements, including the balance sheet, income statement, statement of cash flow, and statement of owner's equity, in conformity with GAAP. The 1933 Securities Act requires companies to provide investors with financial and other important information relevant to securities being offered for public sale. Management is responsible for the accuracy of such information and is liable for fraudulent misstatements. Under the 1934 Securities Exchange Act, companies wishing to sell their shares to the public must prepare registration statements along with financial statements. The management of domestic registrants is responsible for filing an annual report on Form 10-K and quarterly reports on Form 10-Q. The management of foreign registrants must file annual reports on Form 20-F but not quarterly reports.

MANAGEMENT RESPONSIBILITIES UNDER SECTION 302 OF SOX

Senior executives, particularly the chief executive officer (CEO) and the chief financial officer (CFO), are directly responsible for and should assume ownership of internal controls. Section 302 of SOX requires the CEO and CFO or other officers performing in those functions to certify the company's internal controls. The Securities and Exchange Commission (SEC) implemented Section 302 by issuing Rule 33-8124 in August 2002, titled *Certification of Disclosure in Companies' Quarterly and Annual Reports*. This rule defines the new concept of disclosure controls and procedures intended to ensure that information required to be disclosed by the company is recorded, processed, summarized, and reported in a timely manner, enabling management to make appropriate decisions about disclosure. Specifically, the registered company's CEO and CFO must certify in their annual 10-K or quarterly 10-Q filings with the SEC that they have:

- Designed appropriate disclosure controls and procedures to ensure that material information (financial and nonfinancial) has been made known to them
- Designed proper ICFR to provide reasonable assurance with respect to the reliability of financial reporting and fair presentation of financial statements in conformity with GAAP
- Evaluated the effectiveness of the disclosure controls and procedures and disclosed their conclusions regarding their effectiveness as of the end of the reporting period
- Disclosed any change in internal control during the reporting period that could subsequently affect the company's ICFR

MANAGEMENT RESPONSIBILITIES FOR SECTION 404 COMPLIANCE OF SOX

Section 404 of SOX requires management to document and assess the design and operation of the company's ICFR and report on its assessment of the effectiveness of said ICFR. This mandatory internal control report must be integrated into the company's annual reports and include these assertions:

- Management's responsibility for establishing and maintaining adequate and effective ICFR
- The framework used by management in its assessment of the effectiveness of the design and operation of ICFR
- Management's assessment of the effectiveness of the design and operation of the company's ICFR
- Disclosure of any identified material weaknesses in the company's ICFR

- Disclosure that the company's independent auditor has issued an attestation report on management's assessment of the effectiveness of ICFR
- The inclusion in the company's annual report of the independent auditor's attestation report

On June 27, 2007, the SEC issued Interpretive Guidance (IG) and rule amendments to assist public companies in their compliance with Section 404.[2] The IG provides guidance to management on how to conduct an assessment of the effectiveness of ICFR. The IG suggests management use a top-down, risk-based approach in evaluating ICFR and in satisfying the annual evaluation requirement in Exchange Act Rules 13a-15(c) and 15d-15(c). The SEC's IG is focused on two key aspects of ICFR. The first aspect is the design of ICFR. Management is primarily responsible for the effective design and maintenance of ICFR. Management should also evaluate the design of ICFR to determine whether the risk of material misstatements is adequately addressed and whether proper controls are designed to prevent, detect, and correct such misstatements. The guidance suggests the use of a risk-based, top-down approach with a key focus on entity-level controls in the design of adequate controls and in the assessment of the effectiveness of the design in adding financial reporting risks. Management is not necessarily required to identify and document every control in the process but rather must assess the effectiveness of overall controls.

The second aspect of ICFR is its operation. Management is primarily responsible for the effective operation of ICFR and for evaluating ICFR operation based on the assessment of associated risks. The guidance suggests that management use an approach that enables it to obtain evidence to support the effective operation of ICFR, which adequately addresses and evaluates the risk associated with the designed controls. This approach enables management to focus on key control activities that are designed to address the financial reporting errors that pose a greater risk to the quality and reliability of financial reports. Management is therefore provided with more flexibility to obtain and evaluate evidence concerning the effectiveness of the operation of ICFR. Management may choose to reduce self-assessment and cycle testing in low-risk areas and institute more extensive and routine testing in high-risk areas.

INTERNAL CONTROL EVALUATIONS

SEC rules do not specify the methods or procedures that management must use in performing its evaluation of ICFR. Nevertheless, management evaluation should be supported by persuasive evidential matter. Evidential matter consists of adequate documentation of the design, operation, and review of internal control that provides a reasonable basis for the test procedures performed, the evaluation conducted, and conclusions reached. Management's annual assessment of ICFR must be conducted within 90 days of the end of the fiscal year and must be very thorough to permit management reporting on the effectiveness of internal controls. A quarterly evaluation of ICFR must also be performed. However, quarterly assessments do not have

to be as extensive as the annual evaluation. Nevertheless, management must review and evaluate any significant changes in the company's ICFR that occurred pursuant to the annual assessment during a fiscal quarter that has materially affected the company's ICFR, including the corrections of material weaknesses identified by management or the auditor in the evaluation.

SEC rules require public companies to identify the evaluation framework used by the company's management in assuming the effectiveness of ICFR, but the rules do not require the use of a particular evaluation framework. The selected evaluation framework must be a recognized framework established by a body or group exercising diligence and due process and must be tailored to the company's circumstances. The selected evaluation framework must:

- Be free from bias
- Permit reasonably consistent qualitative and quantitative measures of the company's ICFR
- Be sufficiently complete by including all relevant factors that may influence the effectiveness of the company's ICFR
- Be relevant to the thorough evaluation of internal control

The internal control evaluation framework developed by the Committee of Sponsoring Organizations (COSO) in 1992 meets the aforementioned criteria of the SEC for a suitable evaluation framework. It is expected that evaluation frameworks other than COSO's will be developed in the United States and abroad.

NEW INTERNAL CONTROL REPORTS

Executives must:

- Design, operate, and evaluate effective internal controls
- Identify significant deficiencies
- Disclose material weaknesses
- Identify any fraud by employees with significant roles in internal controls
- Indicate significant changes in internal controls in the management's assessment of the internal control report

Adelphia: "Doing Nothing but Trying to Improve Conditions"

Adelphia, founded in 1952 by John Rigas to diversify against declining revenues in his movie theaters, was a cable television company headquartered in Coudersport, Pennsylvania. While the company went public in 1986, the Rigas family retained control over Adelphia through their exclusive ownership of Adelphia's Class B shares that were

convertible into the company's Class A stock. Whenever Adelphia issued Class A shares to the general public, Adelphia would make a corresponding award of Class B shares to the Rigas family so that the Rigases' ownership and majority voting interests would not be diluted. In addition to their controlling ownership of Adelphia, the Rigas family held five of nine seats on Adelphia's board of directors. Rigas family members involved in Adelphia's management included John (founder, chairman, and CEO), son Tim (CFO), son Michael (executive vice president [EVP]), son James (EVP), and son-in-law Peter Venetis, all of whom were board members.

Members of the Rigas family also owned other private companies (Rigas Entities). Adelphia used its own personnel, inventory, trucks, and equipment to provide services to the customers of these companies. One cause of considerable confusion was that Adelphia, its subsidiaries, and the Rigas Entities shared a centralized treasury system organized using cost centers, in which the cash balances of each company were separately maintained.

Between 1996 and 2000, Adelphia, its subsidiaries, and some Rigas Entities entered as coborrowers into a series of credit agreements. By 1999, Adelphia and the Rigas Entities were indebted by more than $1 billion. In 2000, they tripled their outstanding credit obligations. In early 2002, Adelphia disclosed for the first time the extent of the Rigas Entities' coborrowed debt. The disclosure alarmed investors as well as analysts, and Adelphia's board of directors initiated a formal investigation. The findings included the previously undisclosed related party transactions as well as accounting irregularities.

Subsequently, the SEC alleged that the company via its founder, John Rigas, his three sons, and two executives, James Brown and Michael Mulcahey, committed these fraudulent acts:

- Between mid-1999 and the end of 2001, Adelphia fraudulently excluded from the company's annual and quarterly consolidated financial statements over $2.3 billion in bank debt by deliberately shifting those liabilities onto the books of Adelphia's off-balance sheet, unconsolidated affiliates.
- Adelphia, the Rigases, Brown, and Mulcahey created sham accounting transactions backed by fictitious documents to give the false appearance that Adelphia had actually repaid debts when it had simply shifted them to unconsolidated Rigas-controlled entities and created misleading financial statements by giving the false impression through the use of footnotes that liabilities listed in the company's financials included all outstanding debts.
- Timothy and Michael Rigas and James Brown made repeated false statements in press releases, earnings reports, and SEC filings about Adelphia's performance.
- Since at least 1998, Adelphia had made fraudulent misrepresentations and omissions of material facts to conceal extensive self-dealing by the Rigas family. Such self-dealing included the use of Adelphia funds to finance undisclosed open-market stock purchases by the family, purchase timber rights to land in Pennsylvania, construct a golf club for $12.8 million, pay off personal margin loans ($250 million) as well as other Rigas family debts, and purchase luxury condominiums in Colorado, Mexico, and New York City for the Rigas family.

John Rigas was sentenced to 15 years in prison. John's son Timothy, the company's CFO, was sentenced to 20 years in prison. In contrast, James Rigas was never formally charged with criminal violations while Michael Rigas and Michael Mulcahey were not convicted.

(*continued*)

At the height of the fraud, when Timothy discovered the extent of the problems, by some accounts, he limited John's spending to a mere $1 million per month.

Sources: W. Steve Albrecht, "The Adelphia Fraud," AICPA, PowerPoint available from AICPA Web site, 2003 and 2005. "SEC against Adelphia Communications Corporation," John J. Rigas, Timothy J. Rigas, Michael J. Rigas, James P. Rigas, James R. Brown and Michael C. Mulcahey, July 24, 2002, see SEC Litigation Release No. 17627/July 24, 2002. SEC, Litigation Release No. 17627 and Accounting and Auditing Enforcement Release No. 1599, July 24, 2002. Erin McClam, "Adelphia Founder Sentenced to 15 Years," Associated Press/Yahoo! News, June 20, 2005. ACFE Fraud Tools, "Fraud Case Summaries—Adelphia."

MANAGEMENT'S ROLE IN FINANCIAL STATEMENT FRAUD PREVENTION AND PROTECTION

Authoritative reports place primary responsibility for prevention and detection of financial statement fraud with the company's management.[3] The fair presentation of financial statements is the responsibility of management, and accordingly, management is responsible for the prevention and detection of financial statement fraud. In this regard, management has the responsibility, among other things, to complete the following:

- Establish and maintain a sound accounting information system in compliance with GAAP
- Design and implement an adequate and effective internal control system over financial reporting
- Certify the effectiveness of the design and operation of ICFR
- Ensure that the company complies with applicable laws and regulations
- Properly record transactions in accordance with the accounting policies and practices
- Use appropriate and reasonable accounting estimates
- Safeguard assets
- Make all financial records and related financial information available to auditors and fully cooperate with auditors in gathering sufficient as well as competent audit evidence
- Provide fair and full disclosure of financial information and relevant non-financial information
- Serve the interests of investors and creditors by creating and increasing the value of their investments
- Refrain from subordinating judgments to others, under pressure or voluntarily

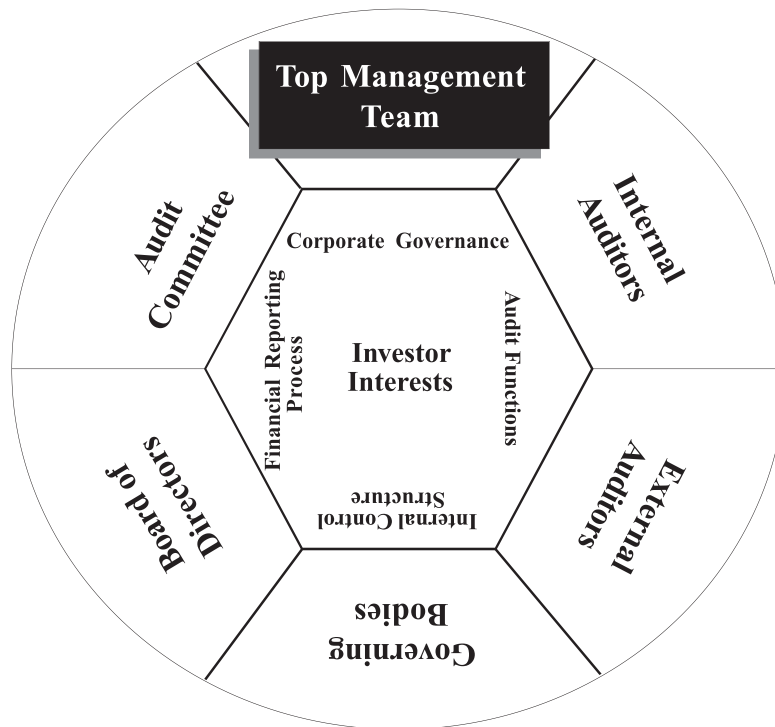


Exhibit 9.1 Corporate Governance and Its Functions

- Ensure that published financial statements are free of material misstatements caused by errors or fraud
- Certify the accuracy and completeness of financial statements
- Comply with authoritative reporting standards promulgated by governing bodies, as depicted in Exhibit 9.1

MANAGEMENT MOTIVES AND INCENTIVES

Publicly traded companies can be motivated by a variety of factors to engage in financial statement fraud. Corporations' rewards and incentive plans, focused on creating shareholder value, motivate management to explore profit opportunities by often operating ‘‘as closely as possible to the borderline between legality and illegality—the borderline between what is ethical and what is unethical [and] for a variety of reasons, an individual manager or management group may cross over the line.’’[4] Management is more likely to cross over the line in five instances:

1. The line is ill-defined.
2. The perceived probable benefits outweigh the probable costs.

3. There is tremendous internal and external pressure to show more favorable performance and financial results.
4. It likes to "live dangerously."
5. It is motivated by a broad variety of other personal satisfactions, prestige, or self-image.

Management may be motivated to engage in financial statement fraud because its personal well-being is so closely associated with the well-being of the company through profit sharing, stock-based compensation plans, and other bonuses; and management is willing to take personal risks for corporate benefit (e.g., risk of indictment or personal, civil, and criminal penalties). Investors' investment preferences and ownership interests can influence management's attitude and operating style. For example, management would be less likely to engage in short-term earnings management if investors show preference for long-term return on their investments. Pressure by investors, especially short-term institutional investors, for favorable financial performance can lead companies to engage in financial statement fraud.

Management is supposed to make decisions in the interest of shareholders. Thus, management is under internal and external pressure to maximize shareholder value:

- There is external pressure on financial executives not only to make "the numbers" each reporting period but to exceed analysts' consensus estimate of earnings.
- Other senior management executives can impose internal pressure on financial executives to manage earnings. Many executive compensation plans that include stock and earnings-based incentives can increase pressure.

MANAGEMENT OVERRIDE OF INTERNAL CONTROL

The risk of financial statement fraud exists in organizations of all sizes and types. This risk can be managed and mitigated where there is effective corporate governance and internal controls; however, such a risk can increase where there is a possibility of management overriding internal controls. The American Institute of Certified Public Accountants (AICPA) antifraud programs and control task force AICPA/APCTF (2002) states that financial statement fraud often occurs when management intentionally overrides internal controls, and thus the audit committee plays an important role in addressing the risk of management override. Management is primarily responsible for the effective design and operation of ICFR. When management has incentives to meet financial targets through earnings management and the opportunities to override ICFR exists, senior executives may engage in financial statement fraud.[5] The report of AICPA/APCTF (2002), while acknowledging that management override of internal controls cannot easily be

detected and prevented, suggests several actions for the audit committee to address the risk of such an override and mitigate its effects. These suggested actions are:

- Maintaining an appropriate level of skepticism
- Strengthening the audit committee's understanding of the business
- Using the code of conduct to evaluate financial reporting culture
- Brainstorming about fraud risks
- Establishing a broad information and feedback network
- Utilizing an effective whistle-blowers program

Exhibit 9.2 illustrates these actions and how they can help in addressing the risk of management override internal controls.

Exhibit 9.2 Risk of Management Override of Internal Controls

Actions	Description
Maintaining skepticism	1. Assuming that the risk of management override exists in an organization 2. Being able to ask difficult, challenging, and straightforward questions 3. Considering alternative scenarios related to the possibility of fraud in the organization during the audit committee meetings 4. Disregarding any beliefs about the integrity of management in the organizations
Strengthening committee understanding of the business	1. Developing a broad and up-to-date knowledge of the business, the industry it operates in, and the management compensation policies adopted in the particular organization 2. Creating a set of possible reactions to the certain variances in financial performance 3. Concentrating on relevant key performance indicators (KPIs) 4. Recognizing potential threats to management's performance 5. Understanding the budgeting process in the organization
Brainstorming to identify fraud risks	1. Exchanging ideas between audit committee members on the override management risk factors 2. Conducting brainstorming sessions with as many affiliates as possible 3. Encouraging the brainstorm participants to be well prepared in advance

(*continued*)

Exhibit 9.2 (continued)

Actions	Description
Using the Code of Conduct to assess financial reporting culture	1. Using a code of conduct as a benchmark 2. Obtaining information from any possible sources regarding the ability of employees and affiliate parties to follow the code of conduct 3. Continually educating employees on the companies' expectations about ethical behavior within the organization
Cultivating a vigorous whistle-blower program	1. Involving suppliers, customers, and others, as well as employees, to participate in the whistle-blowing program 2. Assuring the participants of the program that their concerns will be objectively addressed 3. Providing a strong leadership support from the audit committee, board of directors, and managers 4. Setting a specific program that can route all the complaints involving senior management directly to the audit committee 5. Ensuring the continuous upgrade of the whistle-blowers' process in the organization
Developing a broad information and feedback network	1. Establishing genuine communications with the compensation committee 2. Developing a frank dialogue with key employees within the organization without distracting relations with management

Source: AICPA (2005), ''Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention,''; available at www.aicpa.org/audcommctr/download/achilles_heel.pdf.

GAMESMANSHIP

The global economy and Internet-based technologies have brought new ideas, inventions, and imperatives that significantly affect the business environment. These factors have affected and will continue to affect the quality and integrity of information provided to investors. The desirability and reality of not only meeting but also exceeding investors' earnings expectations are often a challenge for many managers of publicly traded companies. Creating shareholder value has become the primary goal of corporations. In achieving this goal whenever possible, corporate top executives may try every trick in the book to prevent their company's stock price from falling and to ensure they will receive a bonus or retain their position within the company. Although most U.S. companies are attempting to meet market participants' earnings expectations through continuous improvements in both quality and quantity of earnings, some companies have engaged in unacceptable and illegitimate earnings management practices that eventually undermine investors'

confidence in the quality and integrity of the financial reporting process. This unacceptable, unethical, and illegitimate practice of earnings management is viewed by the former SEC chairperson Arthur Levitt as "a culture of gamesmanship" between companies, security analysts, and auditors.[6] The purpose of this game is to "push accounting" guidelines to the limit to create the rosiest profit projections possible to meet analysts' projections and sustain or boost stock prices.

Traditionally this unacceptable and illegitimate earnings management has not been a focus of much scrutiny. Corporate top management teams are now under more pressure to create shareholder value and, in turn, secure their own positions and compensation. The gamesmanship notion motivates management to use its discretion in choosing accounting principles and methods that maximize shareholder value through practices of:

- Overstating restructuring charges and creating a buffer with which to meet future Wall Street earnings estimates
- Using acquisition accounting to overstate future earnings
- Smoothing earnings by manipulating timing recognition of charges such as loan losses and sales returns
- Recognizing sales before completion or when a sale is still reversible by customers
- Overstating revenues and assets
- Deferring expenses to portray earnings growth

Monitoring gamesmanship is a challenge for corporate governance primarily because no one is ever sure what actions someone else will take, and not everyone can resist pressure; however, corporate governance should create safeguards to monitor and prevent gamesmanship in order to secure the quality and quantity of financial reports. Some of the safeguards or monitoring methods to combat unhealthy gamesmanship are vigilant oversight by the board of directors, effective risk assessment, appropriate use of professional judgment in determining the materiality threshold in evaluating financial misstatements, and effective enforcement of auditor independence rules. Management engages in gamesmanship practice by either lowering analysts' and investors' expectations below the level of actual and potential company performance or by tailoring financial reports to match market expectations to prevent any surprises and adverse impacts on stock prices. The board of directors and audit committee should know the company's operations, identify operational and financial risks, and provide safeguards to control their effects on the quality and integrity of financial reports.

Foreign Corrupt Practices Act—A Headache of International Proportions

The Foreign Corrupt Practices Act (FCPA) is one of the most challenging laws faced by America's corporations operating on foreign soil. According to the Department of Justice (DOJ) Web site, the FCPA makes it unlawful to bribe foreign government officials to obtain

(*continued*)

or retain business. The FCPA not only applies to company employees, it also potentially applies to any individual, firm, officer, director, and owner or agent of a firm acting on behalf of a firm. The challenge is that bribery is embedded in the culture of many countries. Given the cultural, social, legal, and jurisdictional issues associated with international operations, and the penalties associated with noncompliance, FCPA is a frightening prospect, even for the most ethical of businesses.

As an example, in October 2006, the DOJ and the SEC announced that Schnitzer Steel Industries, Inc., based in Portland, Oregon, had voluntarily disclosed the payment of bribes to steel mill managers in China and South Korea. As a result of those payments, Schnitzer Steel agreed to a deferred prosecution agreement with the DOJ in addition to a cease-and-desist order with the SEC against future violations of the FCPA. It also agreed to disgorge profits of $6,279,095 and prejudgment interest of $1,446,106. Schnitzer Steel also agreed that its Korean subsidiary would plead guilty and pay a penalty of $7,500,000.

Schnitzer Steel had paid cash bribes and gifts amounting to nearly $1.9 million to managers of both government-controlled and privately owned steel mills in China and to managers of privately owned steel mills in South Korea. Those payments were made in order to induce the managers to purchase scrap metal from Schnitzer Steel. Schnitzer Steel paid "standard" kickbacks out of the revenue it earned on the scrap metal sale. It also paid a second type of kickback whereby the steel mill would overpay Schnitzer Steel for steel purchases and Schnitzer Steel would repay the "overpayment" to the manager of the steel mill as a "refund" or "rebate." Schnitzer Steel wired the payments to the mill managers using secret bank accounts in South Korea. As part of its efforts to influence the mill managers, Schnitzer Steel also gave gifts, including a $2,400 watch and gift certificates worth $10,000.

Schnitzer Steel Industries reportedly learned about its public bribery problem after an employee came back from a company-sponsored FCPA training course. The employee told his supervisors that he and his coworkers were doing all the things the trainers just said were illegal. That triggered Schnitzer's internal investigation, which led to a company clean-up and a favorable settlement with the government.

Sources: William F. Pendergast, Matthew R. Fowler, and Jennifer D. Riddle, "Paul Hastings' Recent FCPA Enforcement Activities" (November 2006). FCPA Blog, September 10, 2008, available at fcpablog.blogspot.com/search/label/Schnitzer.

RISK MANAGEMENT

The purpose of proper risk management is not to eliminate risk but to manage it and to take prudent business risk. Reported financial scandals of Enron, WorldCom, and Parmalat, among others, convey one common theme: the failure of executives and gatekeepers to assess the business circumstances and facts, as well as the related risks and consequences of their decisions and their impacts on the business and all its stakeholders. Compliance with regulation and focus on eliminating risk can divert executive efforts and resources from strategic decisions in creating sustainable shareholder values. In order to improve their performance, companies sometimes fail to assess their risk tolerance appropriately and to integrate risk

management into their business decision making. Companies should optimize their performance through effective risk assessment and management as well as integrate risk tolerance in their corporate culture. Companies should:

- Assess their risk appetite and tolerance and compare it with the industry average risk threshold
- Communicate their risk appetite to all concerned, including shareholders and employees
- Integrate risk management into their strategic decisions, corporate governance, and performance evaluation
- Improve their risk management process and compliance throughout the organization

RISK MANAGEMENT PROGRAMS

A survey shows that over 42 percent of companies admitted gaps in their risk coverage, about 40 percent did not even link risk management to their business strategy, and more than half of their audit committees reported that they do not receive regular risk updates.[7] The company's board, audit committee, and management should consider integrating these four factors in order to assess and oversee their comprehensive risk management program:[8]

1. *Develop an integrated and systematic approach to risk management*. The company's directors and officers should address enterprise-wide, risk-based assessments of their entire organizational and operational structure in order to design and implement a systematic risk management program tailored to their company's strengths and weaknesses.
2. *Clarify ownership risk and risk management*. The company's board of directors is ultimately responsible for ensuring the effectiveness of its risk management. The ownership of the enterprise risk management typically belongs to senior executives. As companies are paying more attention to their risk management programs, it may be appropriate to form a risk committee that provides the board with a greater opportunity to analyze the risk management programs.
3. *Embed a risk culture throughout the organization*. All functions and activities of an organization are subject to risk. Thus, risk should be identified and managed across the entire organization.
4. *Use risk to develop a competitive advantage*. Risk is an integral element of any business, as there is a direct association between risk and reward. This does not mean that management should take an aggressive attitude toward risk. It simply means that management should identify, manage, and take calculated, prudent risks that create the highest rewards and returns. A well-developed risk management program should help in creating shareholder value.

Corporations in the post-SOX period are paying more attention to their risk assessment and risk management policies by considering risk evaluation as an integral part of their decision-making process. The corporate governance listing standards of the New York Stock Exchange require the audit committee to discuss the company's risk assessment and risk management with senior executives. A 2007 KPMG survey reveals that almost half of the 435 surveyed executives want their organization's risk and controls management to assume a more effective, strategic focus to ensure improved and sustained business performance.[9] The most severe barriers in incorporating risk assessment, risk management, and controls into a strategic and forward-looking organization's culture are lack of adequate knowledge of risk management (23 percent) and shortage of resources (17 percent) in effectively managing risk and controls. Survey respondents are taking several initiatives to change their risk and control culture, including:

- 29 (55) percent of respondents expect their organizations to significantly (slightly) increase their risk and control investment and resources
- 43 percent of respondents plan to implement continuous monitoring and auditing
- 56 percent of respondents plan to implement controls transformation, program, and process improvements to effectively align risk and controls with their business needs
- 41 percent of respondents plan to implement organization-wide enterprise risk assessment and management to align risk and controls with their business strategy
- 37 percent of respondents plan to implement executive dashboards to address key events and performance indicators in identifying emerging risks and opportunities[10]

MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROLS

In the post-SOX era, management is primarily responsible for both the fair presentation of financial statements and the effectiveness of internal control over financial reporting. This involves adopting a sound accounting information system that conforms to GAAP in reflecting fair presentation of operating results, financial position, and cash flows; and establishing and maintaining an adequate and effective internal control system to achieve the three categories of control objectives discussed earlier, particularly those related to the reliability of financial statements. In following its internal control responsibilities, management sets a tone at the top that is ethical, aimed at creating and increasing shareholder value, and promotes reliable financial reports. Risk assessment and risk management of operations and financial reports are also the responsibilities of management. The company's information systems should be properly designed, maintained, and supervised by management. In addition, management is responsible for the timely monitoring of the

entire internal control system to ensure that internal control objectives are being achieved and required changes are made as necessary.

MANAGEMENT REPORT ON INTERNAL CONTROLS

Management reports on internal controls are prepared and published to serve a variety of purposes, including:

- To communicate to investors, creditors, and other users of the report the adequacy and effectiveness of the internal control system in ensuring the achievement of the company's objectives
- To discuss the company's efforts to safeguard its resources and reach its strategic goals
- To clarify the role of the audit committee, its functions, responsibilities, and composition
- To emphasize that the company's internal control system provides reasonable assurance regarding achievement of intended goals and objectives
- To describe how the company uses its independent audit services to assist in managing or assessing the internal control system
- To discuss that an adequate and effective internal control system can assist in preventing, detecting, and correcting material misstatements in financial reports caused by errors and fraud

Management should evaluate the identified deficiencies in ICFR by using both qualitative and quantitative factors to determine whether these deficiencies are material weaknesses. The SEC's Interpretive Guidance directs management to consider both the likelihood that a control will fail to prevent or detect a misstatement and the magnitude of the misstatement that might result from the control deficiency. Factors that management should consider in deciding whether there is a reasonable possibility that a deficiency may result in a misstatement in financial statements include:

- The nature of the financial statement items
- The susceptibility of the concerned asset or liability to loss or fraud
- The extent, subjectivity, or complexity of judgment required to determine the amount involved
- The deficiency's interaction with other identified deficiencies
- The association of the control with other controls
- The potential consequences of the deficiency
- The magnitude of the misstatement that may result from the deficiency
- Any other relevant information that may assist in determining whether there is a material weakness

ANTIFRAUD APPLICATIONS FOR PRACTICE

TARGETED RISK ASSESSMENT IN DETAIL

Management has primary responsibility for the company's fraud risk assessments. The company's audit committee (board of directors) is responsible for overseeing management's work in this area and monitoring frauds, including management override that could be perpetrated by management, as well as interacting with internal and external auditors with respect to their efforts to detect material misstatement.

Auditing Standard No. 5 (AS5) of the Public Company Accounting Oversight Board (PCAOB), *An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements*, requires a top-down approach. Targeted fraud risk assessment is consistent with the AS5 guidelines. First, fraud risk factors related to the organization's industry, competition, historical performance, management philosophy, as well as possible pressures and incentives are identified. Then specific fraud risks are considered: what are the likely schemes, what are the related potential costs (magnitude) associated with the scheme, and which accounts will likely be utilized (revenue, expenses, liabilities, assets) to perpetrate the fraud and cover it up. Then consideration is given to those persons most likely to be involved in the scheme. The targeted fraud risk assessment approach correlates the degree of risk that a material misstatement could occur with the amount of attention management needs to devote to that area.[11]

This 10-step approach implements the targeted fraud risk assessment, as described in Exhibit 9.3.[12]

Step 1. *Identify, understand, and evaluate the company's operating environment, as well as the pressures and incentives that exist for persons to commit fraud.* This step evaluates the economic, operating, and competitive environment; the company's business conditions; and the overall control environment.

Step 2. *Identify the business processes and consider differences in those processes across the organization.* This step includes the identification of key business processes, including sales, accounts receivable collections, personnel, payroll, procurement (acquisition), accounts payable, cash disbursements, inventory, warehousing, distribution, capital asset acquisition (including maintenance and depreciation), cash accounting and control, licensing, intellectual property, investing, information and technology, marketing, and research and development. This step also considers differences in the processes identified between local and foreign operations, as well as among subsidiaries or decentralized divisions. Some of the considerations include legal requirements across the various jurisdictions, cultural differences, processes for transaction approval, and the competency of management and supervisors within the organization.

Exhibit 9.3 "Managing the Business Risk of Fraud: A Practical Guide" Captures the Targeted Fraud Risk Assessment

Identified Fraud Risks and Schemes	Likelihood	Significance	Potential Perpetrators: Processes, People and/or Departments	Existing Anti-Fraud Controls	Controls Effectiveness Assessment	Residual Fraud Risks	Fraud Risk Response
Examples from Chapter 5							
Fictitious Customer Revenue[*]							
Invoices to phony companies	**	**	**	**	**	**	**
Phony invoices (other documentation) to legitimate customers							
Shipments to customers without an order							
Shipments to noncustomers (e.g., warehouse location)							
Recording accounts receivable collections as revenue							
Recording deposits as revenue							
Recording supplier refunds as revenue							
Round-trip transactions							
Money laundering							

[*] The fraud risk assessment process includes each of the other potential schemes in the taxonomy outlined in Chapter 5: overstated revenues, understated revenues, premature revenue recognition, expense misstatement, schemes involving assets (cash, accounts receivable, investments, property plant and equipment and intangibles, other current and long-term assets), understated liabilities, overstated liabilities, misstated stockholders equity, related-party transactions and concerns about other forms of recurring and nonrecurring income and expense, misappropriation of assets, and corruption.

[**] These blocks are completed based on the outcomes of the targeted fraud risk assessment process.

Step 3. *Identify the process owner for each of the identified significant processes*. The process owner may be a senior-level executive, subsidiary president, regional president, vice president, manager, or supervisor. The process owner is that individual who has the day-to-day authority and is in a position to alter (override) standard operating procedures. Being in a position to override normal operating procedures means the person can alter those procedures for less than desirable purposes.

Step 4. *Review past fraud experience within the company for the process being evaluated*. This step requires an assessment of the organization's history with respect to fraud as well as the company's fraud experiences at lower levels of the organization by process, geographic locale, and within specific jurisdictions. Consider these types of questions:

- What kinds of fraud have occurred?
- Where (geographically, and in which accounts) did the fraud occur?
- Where within the organizational structure did the fraud occur?
- Who committed the fraud?
- How did the fraud occur?
- How could the fraud have been prevented?
- What methods of early detection could have been used?
- What may have deterred the commission of the fraud?

Step 5. *Identify how fraud may occur in each process at each location using brainstorming techniques*. This step addresses the question: What could go wrong? The brainstorming process should focus on fraud risk factors by process, locale, and jurisdiction, giving consideration to those fraud schemes that would be likely (probable) and significant (of large financial magnitude). Generally, those schemes that are financially significant and likely should be evaluated more carefully. Participants in the brainstorming process should identify control activities that could mitigate the identified fraud schemes, assuming such controls were properly designed and are operational.

Step 6. *Identify the parties who have the ability to commit the potential fraud*. In this step, the identified parties who have the ability to commit the potential fraud need to be examined more closely, considering the elements of the fraud triangle: pressure, opportunity, and rationalization. (See Exhibit 9.4.)

Step 7. *Evaluate the likelihood that each of the identified fraud schemes could be assessed as (a) remote, (b) reasonably possible, or (c) probable*. For each potential fraud, ask the following:

- What is the likelihood of this fraud occurring and being significant?
- How could this fraud manifest itself, and where (which account and which process)?
- What would the fraud look like, and where would I find it?

Exhibit 9.4 Management Fraud Triangle

Incentives/pressure	1. Threat to financial stability caused by change in economic, industry, or entity operating conditions 2. Excessive pressure on management to meet or exceed expectations on performance targets 3. Conflict of interests caused by managerial greediness
Opportunities	1. Nature of the industry. Some industries, due to their nature, are more prone to the risk of fraudulent reporting 2. Past performance. The past is the best predictor of the future 3. Organizational structure. Its complexity and stability 4. Effectiveness of the internal control in the organization
Rationalizations/attitudes	1. Management ability to effectively maintain ethical standards in the organization 2. Management willingness to cooperate with other affiliates in order to prevent fraudulent actions

Source: AICPA "Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention" (2005); available at www.aicpa.org/audcommctr/download/achilles_heel.pdf.

- What is the likelihood of the fraud being perpetrated by two or more individuals acting collusively or overriding the system?

  Management should address those fraud risks that have more than a remote likelihood of having a more than an inconsequential effect on the company's financial statements. The auditor should evaluate all controls specifically intended to address the risks of fraud that have at least a reasonably possible likelihood of having a material effect on the company's financial statements.

Step 8. *Consider the likely methodology to commit* and conceal *the fraud in order to determine the level of mitigation required to prevent, early detect, and deter the fraud.* Then consider the control environment, control activities, information, and communication, in addition to monitoring the design and effectiveness. The result, unmitigated fraud risks, is a determination of the existence of residual fraud risk.

- Are entity level controls in place and operational?
- How effectively is the antifraud message communicated throughout the organization?
- Are there effective fraud awareness training programs?
- Does the organization complete an effective fraud risk assessment?
- Does the organization have effective ethics training and programs?
- What ethics and core values seem to exist within the organization?
- Do employees embrace the ethics and core values, or are they apathetic?

- Does the organization have an effective fraud hotline and whistle-blower protection?
- Are allegations of fraud and wrongdoing investigated timely and completely?
- What control activities are in place?
- What information systems are in place, and does communication happen as designed and in a timely fashion?
- What monitoring activities are in place?
- What effective remediation and fraud investigation processes and procedures are designed and operational?

Step 9 *Investigate the characteristics of potential fraud manifestations within each process identified where residual fraud risk exists*. This step requires additional work: One must investigate the characteristics of potential fraud manifestations within each process identified where residual fraud risk exists. To do so, one must design procedures to look for the fraud (consider data mining techniques) and look for the fraud.

Step 10 *Remediate probable and significant fraud risk schemes by designing control activities to address the unmitigated material fraud risk*. In this step, the results of the work are evaluated and extrapolated to each fraud manifestation over the entire population of possibilities, since any frauds that may have been detected may only be the tip of the iceberg.

The last thought:

> *The public buys the business, but they should have bought the man or men who made the business.*
>
> —Andrew Carnegie

NOTES

1. W. Steve Albrecht, ‘‘The Adelphia Fraud,’’ AICPA, 2005; available at fvs.aicpa.org/Resources/Antifraud+Forensic+Accounting/Educators+and+Students/Integrating+Fraud+Education+Into+the+Accounting+Curriculum/Presentation+Material/Presentation+Materials+on+Fraud+for+Classroom+Use.htm.
2. SEC, *Amendments to Rules Regarding Management's Report on Internal Control over Financial Reporting* (June 20, 2007); available at www.sec.gov/rules/final/2007/33-8809.pdf.
3. National Commission on Fraudulent Financial Reporting (The Treadway Commission), *Report of the National Commission on Fraudulent Financial Reporting* (New York: AICPA, 1987). COSO, *Internal Control-Integrated Framework* (New York: Author, 1992).
4. D. R. Saunders, ‘‘Psychological Perspectives on Management Fraud,’’ in R. K. Elliot and J. J. Willingham, *Management Fraud: Detection and Deterrence* (New York: Petrocelli Books, 1980), 108.

5. AICPA, ''Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention,'' 2005, p. 13; available at www.aicpa.org/audcommctr/download/achilles_heel.pdf.
6. Levitt, A. (1999), ''Quality Information: The Lifehood of Our Market.'' Speech given to the Economic Club of New York City by SEC Chairman on October 18; available at www.sec.gov/news/speech/speecharchive/1999/spch304.htm.
7. Ernst & Young, ''Risk Management Programs: What Does the Audit Committee Need to Know?'' *Board Matters Quarterly* (October 2007); available at www.ey.com/Publication/vwLUAssets/BoardMatters_Quarterly_(2007_October)_risk_management_programs/$FILE/AABS_Assurance_Board_Matters_Quarterly_October2007.pdf.
8. Ibid.
9. KPMG Fraudster Survey 2007; available at www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf.
10. Ibid.
11. The authors are grateful to Steve Silver for his contributions related to targeted risk assessment. Steve Silver retired as a director with Deloitte & Touche, Miami office, in February 2007 and was executive in residence at West Virginia University, 2007–2008.
12. Joseph Wells, Mary-Jo Kranacher, and Richard Riley, *Fraud and Financial Forensics* (Hoboken, NJ: John Wiley & Sons, forthcoming).

Chapter 10

Role of the Internal Auditor

INTRODUCTION

As WorldCom's vice president of internal audit, Cynthia Cooper's odyssey began when she decided to investigate anomalies in WorldCom's accounting entries. According to Cooper, nobody wants to believe that the leadership of a Fortune 500 company is perpetrating a multibillion-dollar fraud. When Cooper showed her evidence to the company's external audit partner, initially he was not concerned. In fact, the audit committee gave chief financial officer (CFO) Scott Sullivan a week-end to write a white paper to support WorldCom's accounting treatment.[1] By the end of June 2002, Cooper and her internal audit team (primarily Gene Morse and Glyn Smith) had blown the whistle on one of the largest corporate frauds in U.S. history: $11 billion.[2] Cynthia Cooper was named one of *Time* magazine's 2002 Persons of the Year for her heroic role as WorldCom whistle-blower.

Since its inception, internal audit has played an integral role in supporting the organizations of which they are a part and the organization's various corporate governance professionals. Internal audit is widely respected as a provider of independent and objective assurance. Internal auditors have made important contributions because of their systematic and disciplined approach to problem solving. They are an important cog in the corporate governance wheel, providing audit services for managers at all levels as well as for the board of directors and the audit committee. Internal auditors' primary responsibility is to assist management at all levels to fulfill their responsibilities by:

- Assessing the efficiency, effectiveness, and economy of organizational performance
- Making constructive suggestions to continuously improve performance
- Monitoring the quality, integrity, and reliability of the financial reporting process

INTERNAL AUDITORS AND CORPORATE GOVERNANCE

Internal auditors are an important part of corporate governance, as depicted in Exhibit 10.1, and are properly positioned to ensure responsible corporate governance and a reliable financial reporting process. Internal auditors' day-to-day

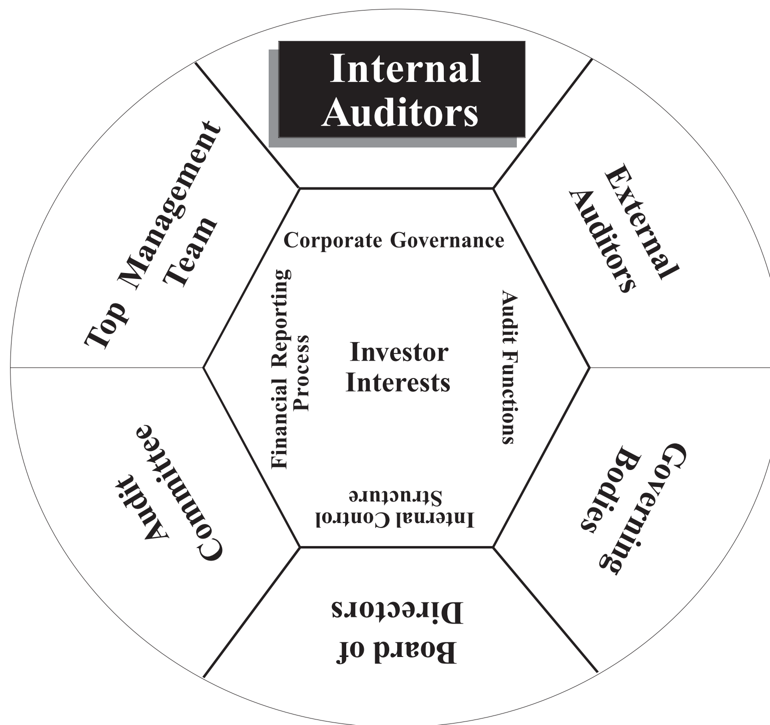


Exhibit 10.1 Corporate Governance and Its Functions

involvement with both operational and financial reporting systems and the internal control structure provide them with the opportunity to perform a thorough and timely assessment of high-risk aspects of the financial reporting process. Internal auditors' responsibility for preventing and detecting financial statement fraud has been extensively disputed in the accounting literature. Nevertheless, the effectiveness of internal auditors to prevent and detect financial statement fraud depends largely on their organizational status and reporting relationships.

Internal auditors play an important role in their company's corporate governance, internal control structure, risk management analysis, and financial reporting process. Internal auditors in the period after the enactment of the Sarbanes-Oxley Act (SOX) of 2002 period have been actively involved in providing management with consulting and assurance services for proper compliance with the provisions of SOX, particularly those provisions related to internal controls, risk assessment, and financial reporting. Internal audit resources have also been expanded to satisfy the demand for internal audit services to assist in executive certifications of internal controls and financial reports. Public companies have recognized the important role internal audits play in effective compliance with Section 404 of SOX and have made several adjustments in response to overwhelming demands for internal audit services. However, internal auditors' services to their organizations go beyond assisting in areas of internal controls, financial reporting, and compliance. Their

traditional roles include the provision of audit services in operational, risk assessment, corporate governance, and nonfinancial activities, as well as quality assurance and improvement programs.

The internal audit function assists management with a variety of issues pertaining to financial reporting and internal controls that impact the company's reliability and effectiveness. Internal auditors, nonetheless, do not provide any assurance regarding the company's financial statements or the effectiveness of internal control over financial reporting (ICFR). Financial statements and ICFR are audited by external auditors, who provide reasonable assurance concerning the reliability and effectiveness of these statements and controls. External auditors should recognize that they may rely on the work of internal auditors in the audit of both financial statements and ICFR, but they are primarily responsible for their audit. Internal auditor status, roles, and responsibilities should be set out formally in the internal audit charter approved by the organization's board of directors. This document should be reviewed and updated by the audit committee as needed to reflect changes in the organization. The audit committee should clearly spell out its expectations of internal auditors and ensure that their independence and objectivity are not compromised at any time.

These risks and their effective assessment, management, and monitoring affect the reliability of financial statements and the effectiveness of ICFR. Internal auditors play an important role in the organization's risk management system and internal controls. Internal auditors can provide assurance to the audit committee and management on the managerial processes designed to manage the risks and minimize their impacts on financial reporting and auditing. The primary role of internal auditors is to provide assurance on the processes designed to manage risk, implement effective internal controls, and produce reliable financial statements. Internal auditors assist the board of directors, management, and external auditors by reviewing and evaluating the effectiveness of the risk management process and internal controls designed to manage the key risks affecting the organization's financial reporting and internal controls.

INTERNAL AUDITORS' RESPONSIBILITIES

Internal auditors must play a proactive role in preventing and detecting financial statement fraud, primarily because of their active involvement in the company's internal control structure and organization status. Unlike external auditors, in theory, internal auditors' effectiveness in preventing and detecting financial statement fraud is not constrained by time budgets and the high costs of expanding their examination of managerial policies and procedures and tests of controls. Internal auditors are in the best position to continuously monitor the company's internal control structure by identifying and investigating red flags that could signal the likelihood of financial statement fraud. Internal auditors' appropriate position in the organizational structure, proper training, knowledge of personnel, familiarity

with managerial policies and operating procedures, and understanding of business conditions and the internal control environment enable them to identify and assess red flags that signal possible financial statement fraud.

The role of internal auditors in preventing and detecting financial statement fraud has been addressed in authoritative reports and professional standards. The Treadway Commission report (1987),[3] for example, recommends that internal auditors take an active role in preventing and detecting financial statement fraud. Statement on Internal Auditing Standards (SIAS) No. 3[4] requires internal auditors to take a proactive role in preventing and detecting financial statement fraud by:

- Identifying qualitative red flags that signal the possibility of fraud
- Investigating symptoms of fraud
- Reporting their findings to the audit committee or other appropriate level of management

Financial statement fraud is often perpetrated by top management teams, who are at the level beyond that which typically is audited by internal auditors. During their normal course of audit, however, internal auditors may become aware of fraud schemes that may affect the quality, integrity, and reliability of financial statements. In such cases, internal auditors should thoroughly investigate the likelihood of financial statement fraud and inform the audit committee regarding the probability of financial statement fraud. Thus, a close working relationship between the audit committee and the internal audit function, particularly private meetings between the chair of the audit committee and the chief internal auditor, can improve the quality of financial statements and reduce the likelihood of financial statement fraud.

A working relationship with external auditors can lead to internal auditors being involved with the financial reporting process at the highest level of consolidation. Thus, through their close coordination and cooperation with external auditors, internal auditors indirectly participate in the final preparation of financial statements. This situation creates an opportunity for internal auditors to take an active role in ensuring the integrity, quality, and reliability of the financial reporting process; further, many organizations and reports—for example, the Blue Ribbon Committee (1999), the Committee of Sponsoring Organizations (COSO; 1999),[5] the Public Company Accounting Oversight Board (PCAOB), Auditing Standard No. 5[6]—encourage internal auditors to take an active role in assessing the quality, reliability, and integrity of the financial reporting process.

The internal auditors' role has evolved in the past several decades from helping management to discharge its responsibilities to assisting the organization to achieve its goals. In addition, internal auditors now perform assurance and consulting services in the areas of corporate governance, risk assessment, internal controls, and financial reporting. The internal audit function can have a very positive impact on the company's internal control structure, the effectiveness of the design and operation of ICFR, the evaluation and testing of the effectiveness of ICFR, and

eventually the reliability of financial statements. The role of internal auditors should be understood and agreed on by the company's board of directors, particularly the audit committee, management, and external auditors. The audit committee should understand and recognize that management is primarily responsible for the fair and true presentation of financial statements and the effectiveness of ICFR. Internal auditors can provide the audit committee with the assurance that ICFR is effective in both design and operation and thus can prevent, detect, and correct misstatements in financial statements on a timely basis. Thus, it is important that the audit committee has confidence in the internal audit function, particularly the chief audit executive (CAE), and can influence the appointment, dismissal, and compensation of the CAE.

Organizations of all types, sizes, and complexity are facing a variety of risks that should be managed through effective risk management systems. Internal auditors can assist in the design and implementation of the organization's:

- Risk management process
- Internal control systems
- Financial reporting process
- Antifraud programs and practices to ensure the integrity of the financial reporting process and ICFR

Internal auditors should conduct themselves in a way that will not threaten their own independence or objectivity and should not put themselves in a position to assess their own work. To maintain their independence and objectivity, internal auditors should:

- Be appropriately positioned within the organization
- Be overseen by the audit committee
- Have reporting lines and adequate resources approved by the board of directors
- Be given unrestricted access to people, records, and information throughout the organization

Best practices of internal auditing suggest the following activities for internal auditors in order to enhance their active role in the financial reporting process and, thus, their role in preventing and detecting financial statement fraud:

- Schedule meetings between the chief internal auditor and the audit committee regarding the financial reporting process
- Establish a consolidated financial statement audit function consisting of the audit committee, internal auditors, external auditors, and the top management team that periodically assesses the quality, reliability, and integrity of the financial reporting process

- Organize close cooperation and coordination of the work of external auditors with internal auditors through an integrated audit planning process consisting of the exchange of audit plans, programs, findings, and reports
- Require that internal auditors report their audit findings related to financial statement preparation, especially when there are indications of financial statement fraud, to the audit committee or the board of directors
- Report to applicable regulatory agencies or even the shareholders when the audit committee fails to act on internal auditors' financial statement fraud findings through a proper whistle-blowing program
- Enhance the status of internal auditors as a part of corporate governance through the higher-level reporting relationship. Provide internal auditors with more access to the audit committee; career development plans for necessary experience, training, and knowledge; and sufficient resources to improve their in the financial reporting process and their effectiveness in preventing and detecting financial statement fraud
- Assess the adequacy and effectiveness of the internal control structure, especially internal controls over the financial reporting process
- Evaluate the quality of the financial reporting process, including a review of both annual and quarterly financial statements filed with the Securities and Exchange Commission (SEC) and other regulatory agencies
- Participate with the audit committee and external auditors in reviewing management's discretionary decisions, judgment, selection, and accounting principles and practices relating to the preparation of financial statements
- Assess the risks and control environment pertaining to the financial reporting process by ensuring that financial reporting risks are identified and related controls are adequate and effective
- Review risks, policies, and procedures, as well as controls pertaining to the quality, integrity, and reliability of financial reporting
- Monitor compliance with the company's code of corporate conduct to ensure that the company is in compliance with ethical policies and other related procedures promoting ethical behavior. The tone set by management in encouraging ethical behavior can be the most effective factor in contributing to the integrity and quality of the financial reporting process

Cynthia Cooper: From WorldCom Internal Audit Manager to *Time*'s ''Person of the Year''

Behind the story of WorldCom are the ethics, dedication, and courage of three internal auditors: Cynthia Cooper, Gene Morse, and Glyn Smith. Based on some initial concerns, a confrontation with CFO Scott Sullivan, a curious e-mail, and an SEC inquiry, in March

(*continued*)

2002, Cooper decided that the internal audit group would start looking at the reliability and integrity of the WorldCom's financial information. By the end of June 2002, Cooper and her internal audit team had blown the whistle on one of the largest corporate frauds in U.S. history: $11 billion.

During their preliminary efforts, the team ran into public disclosure that $2 billion had been spent on capital expenditures during the first three quarters of 2001, despite no documented approvals. Additional work suggested a hypothesis: The mysterious $2 billion might represent operating costs recorded as fixed assets. Cooper and Smith asked Sanjeev Sethi, a director of financial planning, about the curious accounting; Sethi described the capitalized asset as ''prepaid capacity,'' a term Cooper had never heard before. In reality, by 2000, WorldCom had started to rely on aggressive accounting to conceal deteriorating operations. The expenditures were not ''prepaid capacity'' but line lease costs, fees paid to ''rent'' a portion of other companies' telephone networks. Lease line costs were removed from operating expense accounts and buried in the balance sheet as fixed assets. The effect was to improve profits and present a more healthy financial condition for WorldCom.

During May, Gene Morse made another discovery: $500 million in undocumented computer expenses. These expenses had also been recorded as fixed assets.

On June 17, Cynthia Cooper and Glyn Smith began a series of informal confrontations. David Myers, WorldCom's controller, told all: He admitted that he knew the accounting treatment was wrong, electing to end the deception. By the time investigators got to the bottom of the fraud, WorldCom admitted to a $9 billion adjustment for the period from 1999 through the first quarter of 2002.

In the aftermath, the 63-year-old former chief executive Bernie Ebbers was sentenced to 25 years in prison. In addition, Ebbers agreed to forfeit the bulk of his assets, including a $45 million Mississippi mansion, keeping a modest home for his wife and $50,000. Scott Sullivan, CFO, received a five-year sentence. Controller David Meyers and Director of Accounting Buddy Yates were both sentenced to one-year prison terms. Betty Vinson, accounting department manager, was sentenced to five months in prison and five months home detention.

Cynthia Cooper writes: ''Most of the people who participated in the WorldCom fraud were ordinary, middle-class Americans. They were mothers and fathers who went to work to support their families. They had no prior criminal records and never imagined they would be confronted with such life-altering choices.'' Cynthia Cooper was named one of *Time* magazine's 2002 Persons of the Year for her role as WorldCom whistle-blower.

Sources: Cynthia Cooper, *Extraordinary Circumstances: The Journey of a Corporate Whistleblower* (Hoboken, NJ: John Wiley & Sons), 2008. David M. Katz and Julia Homer, ''WorldCom Whistle-blower Cynthia Cooper,'' *CFO Magazine*, February 1, 2008. Corporate Narc, ''Whistle Blower—Cynthia Cooper,'' available at www.corporatenarc.com/cooper.php.

INTERNAL AUDIT FRAUD STANDARDS

SIAS No. 3 describes the internal auditors' responsibility for fraud deterrence as ''examining and evaluating the adequacy and effectiveness of the system of internal control, commensurate with the extent of the potential exposure/risk in the various

segments of the organization's operations."[7] According to SIAS No. 3, internal auditors should identify indicators of fraud and, when deemed necessary, conduct an investigation to determine whether a fraud has actually been committed.

SIAS No. 3 provides guidance relating to the internal auditors' responsibility for deterrence, detection, investigation, and reporting of fraud. Thus, standards clearly state that deterrence of fraud is the responsibility of management. Internal auditors, however, should assess the adequacy and effectiveness of actions taken by management in discharging this obligation. Regarding the detection of fraud, SIAS No. 3 is vague about the responsibility of internal auditors. On one hand, it states that internal auditors should have adequate knowledge of fraud to be able to identify symptoms of fraud and perform audit procedures to detect fraud incidents. On the other hand, it indicates that internal auditors are not expected to have knowledge equivalent to that of a person whose primary responsibility is to detect and investigate fraud, and the routine audit procedures performed by internal auditors are not expected to discover fraud. SIAS No. 3 suggests that fraud investigations be performed by a team consisting of internal auditors, lawyers, investigators, security personnel, and other specialists from inside or outside the organization. Internal auditors have three responsibilities regarding fraud investigation:

1. Determine whether adequate and effective internal controls are in place to discover fraud
2. Design audit procedures to discover similar occurrence of prior-occurring frauds in the future
3. Obtain adequate knowledge of investigating similar fraud

SIAS No. 3 states that internal auditors have four responsibilities for detecting fraud:

1. Internal auditors should obtain sufficient knowledge and understanding of fraud to be able to identify conditions that may indicate the existence of red flags that fraud might have occurred.
2. Internal auditors should study and evaluate corporate structure to identify opportunities, such as a lack of vigilant and effective corporate governance, and weaknesses in internal control structure that could allow the commission of financial statement fraud given the existence of adequate incentives.
3. Internal auditors should evaluate choices made by fraudsters in perpetrating financial statement fraud and decide whether those choices provide further indications (red flags) of fraud and what actions should be taken. The 3Cs factors of conditions, corporate culture, and choices discussed in Chapter 4 should assist internal auditors in identifying the potential fraudulent red flags and developing a risk model to prevent and detect financial statement fraud. Internal auditors' involvement in the routine activities of their organization and internal control

structure place them in the best position to identify and assess indicators (red flags) that may signal financial statement fraud.

4. Internal auditors should inform the appropriate authorities within the organization regarding the possibility of the occurrence of financial statement fraud.

There are two different channels, internal and external, for communicating sensitive issues such as financial statement fraud. The internal channel refers to disclosing fraud to appropriate authorities within the organization, such as top executives, the audit committee, and the board of directors. External channels can be used to communicate fraud to those outside of the organization, including media, external auditors, and authoritative bodies (i.e., SEC). Existing internal auditing standards restrain auditors from disclosing any wrongdoing, including fraud to a party outside of their organizations.

EFFICACY OF INTERNAL AUDIT IN FINANCIAL STATEMENT FRAUD PREVENTION AND DETECTION

Internal auditors can be viewed as a first-line defense against fraud because of their knowledge and understanding of their organization's control structure and business environment. Thus, they are well positioned to prevent and detect all types of frauds, including employee fraud, embezzlement, management, and financial statement fraud. However, there are several reasons to believe that internal auditors may be reluctant to report negative managerial information, such as financial statement fraud, primarily because of the organizational structure and chain-of-command relationships. In most companies, top management teams (e.g., senior management) often make hiring, promotion, performance evaluation, and firing decisions with respect to the chief internal auditors. This may create conflicts of interest in a sense that internal auditors must risk their jobs and careers to report offenses by senior management. Recent corporate governance reforms (SOX, New York Stock Exchange) require the audit committee to be responsible for hiring, compensating, and firing the director of the internal audit department. The internal audit function can protect companies from financial statement fraud when internal auditors are effective in three areas:

1. Preventing financial statement fraud through adequate and effective internal control systems
2. Detecting financial statement fraud by performing internal audit functions
3. Reporting detected financial statement fraud to the top management team and the audit committee

The internal audit function plays a crucial role in preventing and detecting financial statement fraud. Internal auditors, however, are privy to both formal and

informal lines of communication in the company. Accordingly, they are more likely to have a competitive advantage in financial statement fraud detection compared to external auditors. External auditors are constrained by materiality. When combined with time issues, they may not be as effective in identifying the existence of financial statement fraud. With adequate training and the proper position in the organizational hierarchy, internal auditors may be in the best situation to identify and assess symptoms that could signal financial statement fraud. The more routine involvement of internal auditors with business conditions, the financial reporting process, and internal control structure could considerably improve their effectiveness as fraud investigators.

Internal auditors' responsibilities for detecting, investigating, and reporting financial statement fraud, according to their standards (e.g., SIAS No. 3), are to:

- Identify symptoms and red flags that indicate that financial statement fraud may have been perpetrated
- Identify opportunities (e.g., weak internal control, weak audit committee) that may allow financial statement fraud to occur
- Assess the identified symptoms and opportunities, investigate the possibility of their occurrences, and determine actions necessary to reduce or minimize their likelihood of occurring
- Notify the appropriate individuals with the company—top executives if they are not involved in fraud or, otherwise, the board of directors and its representative audit committee—to enable further investigation of the possibility of financial statement fraud

COOPERATION BETWEEN EXTERNAL AND INTERNAL AUDIT

The external auditor is responsible for auditing and attesting to the fair presentation of financial statements, whereas the internal auditor is responsible for monitoring the company's operational and financial performance, as well as the internal control structure. The audit committee should ensure that activities of internal and external auditors complement each other, that their audit functions are coordinated, and that there is open and effective communication between both audit groups. To improve audit effectiveness and efficiency, external auditors should identify internal audit activities that are relevant to planning the audit of financial statements and, if appropriate, rely on the work of internal auditors in determining the nature, timing, and extent of audit procedures.

Internal auditors are in a unique position to cooperate with external auditors and coordinate their audit activities pertaining to audit of internal control over financial reporting (ICFR) as required by Section 404 of SOX. Recent corporate governance reforms, including SOX, SEC rules, and particularly PCAOB auditing standards,

encourage close cooperation between internal and external auditors. External auditors should evaluate the objectivity and competence of internal auditors when considering and accepting documents prepared by internal controls under ICFR. Evidence provided by the internal auditor, along with external auditors' further review and testing, should be used as persuasive evidence to support opinions on financial statements and ICFR. Under no circumstances can external auditors share responsibility for audit decisions and opinions relevant to ICFR.

A 2007 survey of internal controls reveals the following:

- More than 62 percent of internal auditors are communicating more frequently with the external auditors.
- About 45 percent of internal auditors said they are meeting with the external auditors on at least a monthly basis.
- More than half of surveyed internal auditors feel the coordination between internal and external auditors is either minimal or lacking.[8]

Effective cooperation and coordination between external and internal auditors not only reduces the cost of the audit but also improves audit efficiency and quality. Nonetheless, any audit document and evidence prepared by internal auditors should be further reviewed by external auditors to be considered as persuasive evidence to support external auditor opinions on either ICFR or financial statements.

MCI: The Fraud That WorldCom Acquired!

Walter Pavlo, Jr., convicted felon, and *Forbes* magazine senior editor Neil Weinberg in their book *Stolen without a Gun,* describe two frauds: WorldCom's and an embezzlement scheme. In the aftermath of both, WorldCom had to write off at least $500 million in uncollectible receivables and Pavlo pleaded guilty for his role in stealing $6 million and laundering it to the Cayman Islands. According to BDO Seidman, LLP's "White Collar Crime . . . The Road to Prison," the benefit of the financial statement fraud accrued to MCI and the embezzlement of $6 million benefited Pavlo and his co-conspirators.

MCI Accounting Fraud

With regard to MCI's financial statements, Walt Pavlo Jr.'s responsibility was to oversee collection of accounts receivable from long-distance resellers with limited credit histories who earned MCI unusually high margins (before collectability issues were considered). Pavlo realized that much of his customers' debt would be extremely difficult to collect. Despite his pleading with senior management to write off uncollectable accounts and limit marketing's ability to sign these types of customers, Pavlo said that MCI management did not listen. While he had misgivings about the accounting treatment, he felt that he was being a good corporate citizen. Some of the tricks, tools, and techniques that he employed were the following:

- Issuing promissory notes to customers where no collectability was expected and removing the accounts from the aged accounts receivable records

(*continued*)

- Using unapplied cash receipts to reduce delinquent accounts receivable balances
- Accelerating unsigned contract credits and delaying credits on contracts that had been signed
- Recording payments to a fictitious account based on the concept of the check is in the mail

Shifting from Accounting Fraud to Embezzlement

Pavlo indicated that his frustrations led him to take advantage of the chaos surrounding his accounts receivable collection schemes (the accounting fraud). Pavlo worked with an outside co-conspirator, Harold Mann. In just six months, Pavlo, Mann, and at least two other MCI insiders directed seven customers to pay more than $6 million into an account in the Cayman Islands. Because Pavlo's job was collections and Mann was external to MCI, the two used accounting personnel at MCI to conceal the theft.

Pavlo indicated that the pressure of the combined frauds was incredible and noticeable to his wife, family, and friends. He was always concerned with how to keep it hidden. Living a double life, he had no one to confide in; According to the fraud triangle, Pavlo had a nonsharable financial problem. As the fraud unraveled, an internal investigation was launched. Later Pavlo received a "target letter" from the Federal Bureau of Investigations and eventually agreed to plead guilty and go to prison, where he spent 24 months. According to Pavlo, telling his wife and young children that he was going to prison was the most difficult task of his life.

Source: Walter Pavlo Jr. and Neil Weinberg, *Stolen without a Gun: Confessions from Inside History's Biggest Accounting Fraud—the Collapse of MCI Worldcom* (Tampa, FL: Etika Books, 2007); BDO Seidman LLP, "White Collar Crime . . . The Road to Prison," 2008.

INTERNAL AUDITS AND THE AUDIT COMMITTEE

The Treadway Commission[9] recommended that the audit committee get more involved in the internal auditing process by overseeing all internal auditing activities. The commission made four recommendations, suggesting that the audit committee:

1. Effectively and vigilantly oversee the company's internal control
2. Review the appropriateness of the corporate code of conduct and company compliance with it
3. Review any second opinion sought by management on accounting issues and estimates
4. Oversee the quarterly reporting process

Thus, an internal audit function can be a valuable resource to the audit committee in fulfilling its responsibility. To perform their duties most effectively, the

audit committee and internal auditor must work closely and should maintain an open line of communication. The chair of the audit committee and the director of the internal audit department in particular should have unrestricted access to each other.

The audit committee should perform these internal audit functions:

- Participate in the appointment, promotion, replacement, reassignment, or dismissal of the director of the internal audit function
- Concur in the establishment of the internal audit function's goals and mission
- Review the activities and organizational structure of the internal audit department
- Review the findings and results of the internal audit function and management's responses to the internal auditor's findings and recommendations on internal controls
- Review the effectiveness of the internal audit department in carrying out its responsibilities
- Ensure that the internal audit function's involvement in the financial reporting process is appropriate, adequate, and effective
- Ensure that the internal audit department's applied standards and procedures are in compliance with those established by the Institute of Internal Auditors (IIA)
- Review the organizational independence and reporting relationships of the internal audit function
- Ensure that the internal audit department's staffing and budget are adequate, so it is able to carry out its assigned responsibilities

INTERNAL CONTROL

Management is responsible for establishing, maintaining, monitoring the internal control structure, and, in the post-SOX era, reporting on the effectiveness of ICFR. The COSO report defines internal control as:

> 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 three categories:
>
> 1. Effectiveness and efficiency of operations
> 2. Reliability of financial reporting
> 3. Compliance with applicable laws and regulations[10]

Many view this as the most comprehensive definition of internal control, addressing its four major elements of internal control:

1. Process
2. Individuals who affect the internal control and are affected by internal control
3. Limitations of internal control provisions of "reasonable assurance"
4. Objectives categories

The main critique of this definition came from the General Accounting Office (GAO) and the SEC, which stated that the COSO definition does not sufficiently address controls pertaining to the safeguarding of assets, as required by the Foreign Corrupt Practices Act of 1977. Thus, an addendum to "Reporting to External Parties" of the COSO report was published in May 1994 that addresses the safeguarding of assets objectives of internal control.

COMPONENTS OF INTERNAL CONTROL

COSO 1992 defines the five interrelated components and internal control as the following:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring

The control environment consists of the following:

- Integrity
- Ethical values
- Organizational structure
- Management philosophy
- Operating style
- Competent personnel
- Human resource policies and practices
- Assignment of authority and responsibility
- Oversight function of the board of directors and its audit committee

The COSO report emphasizes risk assessment, particularly as it relates to the financial reporting process. Management should assess the information risk that financial statements may be inaccurate, biased, or incomplete, and manage this information risk to a prudent level. Management should also perform a risk analysis of both external and internal factors affecting the integrity and quality of the financial reporting process.

Control activities defined by the COSO report include all managerial policies and procedures designed to ensure that control objectives are achieved. Control activities related to the financial reporting process are intended to prevent, detect, and correct misstatements in the financial statements caused by errors, irregularities, and fraud.

The information and communication component of internal control involves the process of capturing, analyzing, and disseminating relevant information to ensure that personnel receive proper instructions and carry out their assigned responsibilities effectively and efficiently.

The monitoring component of internal control requires continuous assessment of the adequacy, effectiveness, and quality of the internal control system. Any discovered errors, irregularities, and frauds should be reported to top management, as well as to the audit committee, and corrected promptly.

Essential components of an adequate and effective internal control structure that help in preventing, detecting, and correcting financial statement fraud include:

- Commitment from the top management team
- A control environment reflected in the structure, functions, and risks of the company
- Control activities designed to achieve the control objectives of enhancing reliability of financial reporting, improving effectiveness and efficiency of operations, and promoting compliance with applicable laws and regulations
- Continuous and periodic monitoring to ensure the adequacy and effectiveness of the internal control structure
- Communication of the established control activities, policies, and procedures to affected individuals within the corporation
- Proper implementation of control activities and enforcement of control policies and procedures

Internal auditors are well positioned to make recommendations to management regarding the design, implementation, and maintenance of effective internal controls by:

- Developing and maintaining an internal control system that is adequate and effective in managing risks
- Improving the efficiency and effectiveness of risk management processes and controls
- Reviewing entity-level controls relevant to the company's integrity and ethical values, management's philosophy and operating style, organizational structure, human resources policies and procedures, competence and integrity of personnel, and assignment of authority and responsibility
- Challenging management's decisions pertaining to internal control where appropriate

- Facilitating improvements in the internal control structure by working with the company's board of directors, audit committee, and management

In the post-SOX era, demands for internal audit services to actively comply with Sections 302 and 404 on internal control have increased significantly. Internal auditors assist management in documenting, evaluating, testing, and monitoring its ICFR. The audit committee and management rely heavily on internal auditors to assess and document internal controls, and internal auditors are well trained and qualified to tackle SOX challenges. This focus on SOX compliance has diverted the resources and attention of internal auditors from traditional risk-based auditing. Internal auditors add value to their organizations by adopting an all-inclusive approach to audit, risk assessment, and risk management that results in shareholder value creation and enhancement in addition to expanding their audit activities beyond a mere focus on controls.

The IIA, which promotes internal auditors worldwide and provides standards of practices for internal auditors, believes that internal auditors in many public companies are assuming far broader SOX responsibilities.[11] The IIA recommends internal auditors' involvement with Sections 302 and 404 in the four following areas:

1. Project oversight
2. Consulting and project support
3. Ongoing monitoring and testing
4. Project audit

The IIA believes that the internal auditors' roles in Sections 302 and 404 beyond the recommended four areas may impair auditor objectivity, particularly when internal auditors serve as consultants. However, internal auditors can provide training and information to management and other personnel regarding internal controls without compromising their functional objectivity. A 2007 PricewaterhouseCoopers survey indicates that even two years after the initial implementation of Section 404, in the majority of companies (over 64 percent), internal audit leads the way in Section 404 testing, including process test design, management testing, walk-through tests, and process documentation.[12]

Section 302 of SOX requires quarterly management certifications of both financial statements and financial reporting controls, whereas Section 404 requires annual management assessment of the effectiveness of both the design and operation of ICFR. While management's responsibilities for compliance with both Sections 302 and 404 cannot be delegated or abdicated, internal auditors can considerably assist management in fulfilling their compliance responsibilities. When assisting management, internal auditors should maintain their objectivity and independence according to their charter and properly communicate with the audit committee. The CAE (the director of the internal audit department) should consult with the audit committee in devoting internal audit resources to Sections 302 and 404 without

compartmentalizing their other internal audit activities while adding value to their organization's performance. Management is responsible primarily for the design, implementation, and maintenance of ICFR, while internal auditors provide assurance and consulting services. The IIA's 2004 position paper presents:[13]

- The Section 404 compliance process
- Several phases of this process
- Activities within each phase
- Accountability for each activity
- Individual(s) responsible for carrying out each activity
- Recommendations for the internal auditor's role for each activity

The position paper specifies that services performed by the company's internal audit function in assisting management compliance with Sections 302 and 404 of SOX must be consistent with internal auditors' professional standards and should not interfere with their professional obligations to maintain their independence and objectivity. It also recommends project oversight, consulting and project support, ongoing monitoring and testing, and project audit.

The extent of internal auditors' involvement with Sections 302 and 404 depends on the company's internal auditing function, resources, funding, personnel qualifications, and charter. Any activities performed by internal auditors should be in compliance with their charter, professional standards, and mission of adding value to their organization's operations. The IIA's 2004 position paper suggests these points:

- Consulting management on internal control activities compliance does not impair the internal auditor's independence and objectivity.
- Making key management decisions in the compliance process impairs the internal auditor's objectivity and independence.
- Having responsibility for specific operations or participation in directing key management decisions impairs the internal auditor's objectivity and independence.
- Designing, implementing, and drafting procedures for internal controls to comply with Sections 302 and 404 impair the internal auditor's independence and objectivity.
- Recommending standards for internal controls or reviews of internal control procedures does not impair the internal auditor's objectivity and independence.
- Devoting a significant amount of effort to consult with management on Sections 302 and 404 compliance can deplete internal auditors' resources and turn their attention from other value-adding activities.

The IIA has supported the emerging corporate governance, worked with the SEC and PCAOB to find ways to most effectively implement these reforms, and

gathered information from a survey of more than 1,900 CAEs regarding SOX implementation. Based on the findings of this survey, the IIA has made several recommendations to the SEC and the PCAOB to improve Section 404 compliance.[14] Recommendations to the SEC are as follows:

- The importance of enterprise-wide risk management in improving corporate governance rather than just ICFR should be considered.
- More detailed guidance regarding management's assessment of internal controls is necessary.
- More detailed guidance on the quarterly Section 302 management assessment process and the reporting of management corrections of reported material weaknesses is required.
- Clarification of ''principal evidence'' and additional guidance regarding key issues such as a vigilant board of directors and management overrides is needed.
- An increase in the cost effectiveness of compliance with provisions of SOX by clarifying SEC implementation rules and providing better communication between the audit committee, external auditors, and management.
- An appropriate balance between the focus on compliance with Section 404 and other enterprise-wide risks affecting all aspects of corporate governance must be created.

IIA's recommendations to the PCAOB are:

- Increase reliance on the work of others (internal auditors) in the testing of management's assessment of the effectiveness of ICFR.
- Consider partial reliance on the results of the internal control tests from prior years, particularly if there have not been significant changes in the design and operation of ICFR.

The proposed redrafted IIA 610, titled ''The Auditor's Consideration of the Internal Audit Function,'' specifies four key points:

1. The relevance of the internal audit function to the external auditor
2. The extent to which the external auditor should utilize the work of the internal audit function in an integrated audit
3. The risk assessment procedures that should be performed to obtain sufficient understanding of the role of internal audit in internal control
4. The audit procedures necessary when trying to decide whether to use the work of the internal audit function as audit evidence[15]

The independent auditor should determine how the work of the internal audit function could affect the nature, timing, and extent of audit procedures performed in gathering sufficient competent evidence.

INTERNAL AUDITOR ROLES IN ENTERPRISE RISK MANAGEMENT

Enterprise risk management (ERM) has received considerable attention due to its role in addressing challenges, opportunities, risks, and rewards facing organizations of all types, sizes, and complexities. As focus on the risk management concept is widening, it is important to clarify the roles and responsibilities of those who are directly involved with the organization's enterprise-wide risk management process, including the audit committee, management, and internal auditors. Obviously, management is directly responsible for the adequate design and effective operation of the company's risk management process and appropriate risk assessment associated with the process. The audit committee is responsible for overseeing management policies, programs, procedures, and guidelines pertaining to corporate risk management activities. Internal auditors should report to the audit committee that:

- Management has adequately identified and effectively controlled risk.
- Risk management policies and procedures are adequate and effective in addressing the related risk.
- Objective assurance is provided regarding the effectiveness of the company's risk management process.

The IIA issued a position paper, in 2004, titled "The Role of Internal Audit in Enterprise-Wide Risk Management."[16] This paper provides guidance for internal auditors in the ERM environment of providing assurance and consulting services to their organizations while maintaining their objectivity and independence. The primary role of internal auditors is the following:

- Provide assurance to the company's board of directors, particularly the audit committee, on the effectiveness of ERM activities
- Assist in ensuring the proper management of key business risks and the effectiveness of the internal control system
- Advise management in the area of risk assessment and management by providing supporting documentation assessing the risk without making risk management decisions, which is primarily management's responsibility

Internal auditors should assess a potential ERM activity to determine whether the activity is likely to strengthen the company's risk management control and governance structure or internal activities actively raise any threats to their professional independence and objectivity.

Internal auditors are focusing more on effective risk assessments and the use of a risk-based approach in their audit coverage by:

- Adopting a process approach to risk assessment and planning

- Supplementing annual risk assessments with quarterly or more frequent updates
- Leveraging prior assessment results
- Aligning risk assessments
- Obtaining the needed specialized talent
- Coordinating with other risk management groups[17]

Effective involvement of internal auditors with ERM can strengthen risk assessment that reduces incentives and opportunities for the occurrence of financial statement fraud.

ANTIFRAUD APPLICATIONS FOR PRACTICE

In a post-SOX environment, the role of internal audit is even more critical than it has been in the past. One of internal audit's key roles with respect to fraud is evaluating and improving the effectiveness of fraud risk management, prevention, deterrence and detection controls, and critically evaluating governance processes with respect to fraud. Maybe most significant is the special and important role of internal audit with respect to concerns of management override and collusive fraud detection.

More specifically, internal audit's integral role and responsibility can be carried out in these six areas:[18]

1. Key characteristics of an effective internal audit group:
   - Reports to the audit committee or in such a manner so as to be considered independent of management
   - Is properly trained and professionally qualified in fraud risk assessment, fraud schemes and fraud prevention, deterrence, and detection
   - Has sufficient knowledge, training, and experience with regard to the red flag symptoms of fraud schemes
   - Has a commitment to design audit plans based on fraud risk assessments
   - Uses brainstorming techniques as part of risk assessment
   - Is professionally skeptical
   - Is unpredictable
   - Responds to concerns over allegations and suspicions of collusive behaviors and management override
   - Is committed to evidence-based decision making, including the use of non-financial data and information
2. Internal audit's role in the critical evaluation of the organization's antifraud measures:
   - Assesses fraud risks: evaluating, reviewing, and auditing management's fraud risk assessment

- Because internal controls alone are insufficient, internal audit assesses the organization's culture to verify that the organization:
  - Is aware of internal controls, their purpose, and the consequences of inadequate or nonfunctional internal controls
  - Has goals, objectives, strategies, operational plans, and budgets
  - Has written policies that prescribe ethical behavior and outline prohibited activities
  - Has written policies that require appropriate responses when policy violations are alleged
  - Has appropriate policies for transaction approval
  - Has appropriate monitoring (e.g., supervision) activities
  - Has appropriate asset safeguards
  - Has effective and operational communication options, including tips and complaints hotlines
  - Provides adequate and reliable information for the board, audit committee, senior management, managers, supervisors, line employees, and staff

3. Internal audit conducts surveys to measure the organization's ethical environment:

- The propensity for wrongdoing
- The likelihood that persons observing ''bad behavior'' will report it
- The belief that management will support whistle-blowers
- The belief that whistle-blowers would suffer retribution or punishment for their actions
- Appropriate hiring and employee screening processes

4. Internal audit assesses fraud detection activities:

- Reviews and audits the fraud tip hotline:
  - Design
  - Scope: employees, customers, suppliers, and vendors
  - Operations: Does it work according to plan?
- Evaluates, reviews, and audits management's system of antifraud controls for prevention and detection:
  - Design
  - Implementation

5. Internal audit is part of the ''perception of detection.'' It lets the board of directors, audit committee, senior management, managers, supervisors, line employees, and staff know that internal audit:

- Is looking for fraud

- Welcomes tips, complaints, allegations, and information regarding suspicions of fraud
- Asks tough questions of management and employees (for examples, see suggested questions in Chapter 8)

6. Internal audit conducts timely investigations of allegations and suspicions of fraud acts, including those associated with collusive behavior and management override.

Last thought:

People don't wake up and say, ''I think I'll become a criminal today.'' Instead, it's often a slippery slope and we lose our footing one step at a time.

—Cynthia Cooper, *Extraordinary Circumstances*

NOTES

1. Cynthia Cooper, *Extraordinary Circumstances: The Journey of a Corporate Whistle-blower* (Hoboken, NJ: John Wiley & Sons), 2008.
2. David M. Katz and Julia Homer, ''WorldCom Whistle-blower Cynthia Cooper,'' *CFO Magazine*, February 1, 2008.
3. National Commission on Fraudulent Financial Reporting (The Treadway Commission), *Report of the National Commission on Fraudulent Financial Reporting* (New York: AICPA, October, 1987); available at www.coso.org/publications/NCFFR.pdf.
4. Institute of Internal Auditors, *Statement of Internal Auditing Standards No. 3: Deterrence, Detection, Investigation and Reporting of Fraud* (Altamonte Springs, FL: Author, 1985); available at aaahq.org/audit/midyear/02midyear/papers/1-16-02%20Draft.doc.
5. Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees, *Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees* (New York: NYSE and NASD, 1999). M. S. Beasley, J. V. Carcello, and D. R. Hermanson, *Fraudulent Financial Reporting: 1987–1997, An Analysis of U.S. Public Companies* (New York: COSO, 1999).
6. PCAOB Auditing Standard No.5; available at www.pcaobus.org/Rules/Docket_021/2007-05-24_Release_No_2007-005.pdf.
7. IIA, *Statement of Internal Auditing Standards No. 3.*
8. IIA, *Re: Implementation of U.S. Sarbanes-Oxley Act Internal Control Provisions* (March 31, 2005); available at www.theiia.org/download.cfm?file=73806.
9. NCFFR, *Report of the National Commission on Fraudulent Financial Reporting*. (October, 1987); available at www.coso.org/publications/NCFFR.pdf.
10. COSO, *Internal Control-Integrated Framework* (New York: COSO, 1992); available at www.coso.org/documents/VolumeI-ExecutiveSummary.pdf.
11. IIA, *Internal Auditing Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002* (May 26, 2004); available at www.theiia.org/download.cfm?file=1655.

12. PricewaterhouseCoopers, *State of the Internal Audit Profession Study: Internal Audit Post-Sarbanes-Oxley* (May 2007); available at www.pwc.com.
13. Internal Institute of Auditors. ''The role of Internal Auditing in Enterprise-Wide Risk Management,'' September 29, 2004; available at www.ucop.edu/riskmgt/erm/documents/erm1.pdf.
14. IIA, *Re: Implementation of U.S. Sarbanes-Oxley Act Internal Control Provisions*.
15. International Auditing and Assurance Standards Board, *ISA 610: The Auditor's Consideration of the Internal Audit Function* (December 22, 2006); available at www.ifac.org/Guidance/EXD-Details.php?EDID=0073.
16. IIA, *The Role of Internal Audit in Enterprise-Wide Risk Management* (September 29, 2004); available at www.theiia.org/download.cfm?file=283.
17. PricewaterhouseCoopers, ''Advisory Internal Audit, PricewaterhouseCoopers,'' *State of Internal Audit Profession Study: Pressures Build for Continual Focus on Risk* (2007); available at www.pwc.com/internalaudit.
18. Steve Stanek, ''Internal Audit's Role in Fraud Prevention,'' Protiviti's KnowledgeLeader Internal Audit and Risk Management Community. IIA, AICPA, and ACEF (April 26, 2004), *Managing the Business Risk of Fraud: A Practical Guide* (2008); available at www.acfe.com/documents/managing-business-risk.pdf.

Chapter 11

Role of External Auditors

INTRODUCTION

About 1915, Arthur Andersen—*the* Arthur Andersen—was confronted with a difficult situation with respect to the financial statements of a Midwestern inter-urban railway company. The company had ''distorted'' its earnings by capitalizing relatively large charges (expenditures) that should have been absorbed as current operating expenses in the income statement. Andersen was insistent that the financial statements to which he attached his report disclose the facts. The president of the company, an autocratic man who was accustomed to having his own way, went to Chicago and demanded that Arthur Andersen issue a report approving the company's procedure in deferring these operating charges. Andersen's response: ''There is not enough money in the city of Chicago to make me change this report.'' Andersen lost the client at a time when the firm was small and the loss of a client was almost a life-and-death matter. His decision was vindicated when a few months later; the railroad company was forced to file a petition in bankruptcy.[1]

Users of audited financial statements, particularly investors and creditors, traditionally have held independent auditors responsible for detecting financial statement fraud. Independent auditors, however, in compliance with their professional standards, provide only reasonable assurance that financial statements are free of material misstatements, whether caused by error or fraud. This chapter presents external auditors responsibilities in auditing financial statements, the role of independent auditors in detecting financial statement fraud, characteristics of high-quality financial audits, independent auditors' report on internal control, and methods of improving audit effectiveness.

INDEPENDENT AUDIT OF FINANCIAL STATEMENTS

The capital markets function efficiently when market participants, including investors and creditors, have confidence in published financial statements and related audit functions. An increasing number of restatements and alleged financial statement fraud committed by high-profile companies has eroded public confidence in the financial reporting process and audit functions. Some of the defining characteristics of the accounting profession are its integrity, objectivity, independence, and trust. The public trust in auditors' judgments is the cornerstone of our profession.

Several initiatives have been taken by Congress (e.g., the Sarbanes-Oxley Act [SOX]), regulators (Securities and Exchange Commission [SEC]), and the accounting profession (Public Company Accounting Oversight Board [PCAOB], American Institute of Certified Public Accountants [AICPA]) to restore public confidence and trust in financial reports and related audits.

In the early years of the auditing profession in the United States, from 1850 through the early 1900s, the primary purpose of the audit was to detect fraud, errors, and intentional misstatements. The Industrial Revolution and the substantial growth in public companies and their transactions caused a shift away from verifying all business transactions in order to discover fraud to determining the fair presentation of financial statements. Today auditors' responsibilities are to provide reasonable assurance about fairness in financial reporting rather than detecting fraud. This notion of reasonable assurance has widened the gap between society's expectations of auditors and auditors' responsibilities and performance. In the auditing profession, the so-called expectation gap is the difference between (1) what the investing public and other users of audited financial statements believe auditors' responsibilities are and (2) what auditors are willing to assume as responsibilities according to their professional standards. For example, the public desires to hold auditors responsible for all fraudulent activities involved in public companies' financial reports; auditors, however, only provide a reasonable assurance that financial statements are free from material misstatements, whether caused by error or fraud.

Current auditing standards require that independent auditors provide *reasonable assurance* that the financial statements are free from material misstatements, whether caused by error or fraud, in order to render an unqualified (clean) opinion on the financial statements. This level of reasonable assurance is regarded as a high level of assurance but not absolute assurance. Reasonable assurance may mean different levels of assurance to different groups. Investors in the post-Enron era expect independent auditors to discover and report on all material misstatements, including errors, irregularities, and fraud. Independent auditors, however, in complying with their professional standards, provide reasonable assurance that financial statements are free from material misstatements. The central issue vital to the audit quality is the nature and extent of auditors' responsibility to detect financial statement fraud. Nevertheless, there is a widening expectation gap between what auditors should be doing and what auditors are willing to accept and are capable of doing to discover fraud according to their standards of auditing and the fees collected for their service.

Auditors are not expected to provide absolute assurance for detecting fraud, but they have been blamed when high-profile financial scandals resulting from fraudulent activities occur. The U.S. Chamber of Commerce called on the PCAOB to issue safe harbor auditing standards on fraud detection to "better define an auditor's procedures for fraud detection and the limit of an auditor's responsibility."[2] The AICPA, on two other occasions, attempted to further address the expectation gap by issuing Statement on Auditing Standards (SAS) No. 82 and subsequently SAS No. 99, *Auditors' Consideration of Fraud in a Financial Statement Audit*.[3] However, these standards have not reduced the perceived expectation gap in the areas of internal control,

transparency of disclosures, fraud, and illegal operations. Now it is up to the accounting profession, particularly the PCAOB, the "public watchdog," to undertake appropriate measures to narrow the perceived expectation gap. To reduce this expectation gap effectively, the PCAOB needs to reexamine the primary role of auditors in the area of fraud detection and society's understanding of the real meaning of "present fairly" according to generally accepted accounting principles (GAAP).

External auditors opine on the fair presentation of financial statements in conformity with GAAP, and thus they are responsible for the content of their report. Although management is primarily responsible for the fair presentation of financial statements in conformity with GAAP, the auditor's report attests to the fairness of management presentations and/or assertions. Exhibit 11.1 presents an example of the auditor's unqualified report. This report states that the financial statement, including the notes, present fairly, in all material respects, the financial position, the results of operations, and the cash flows for the reported accounting period, in conformity with GAAP. This unqualified report provides reasonable assurance that the published audited financial statements are free of material misstatements caused by errors and fraud; however, some circumstances warrant audit reports other than an unqualified opinion (e.g., modified unqualified, qualified, disclaimer, adverse).

Exhibit 11.1 Report of Independent Registered Public Accounting Firms

We have audited the accompanying balance sheets of X Company as of December 31, 20X3 and 20X2, and the related statements of operations, stockholders' equity, and cash flows for each of the three years in the period ended December 31, 20X3. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the Company as of [at] December 31, 20X3, and 20X2, and the results of its operations and its cash flows for each of the three years in the period ended December 31, 20X3, in conformity with U.S. general accepted accounting principles.

[*Signature*]

[*City and State or Country*]

[*Date*]

Source: Adapted from the Public Company Accounting Oversight Board, "Auditing Standard #1: References in Auditors Reports to the Standards of the Public Company Accounting Oversight Board," May 24, 2004; available at www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.1.aspx.

The auditor's report on financial statements usually covers the company's four basic financial statements—balance sheet, income statement, statement of cash flow, and statement of owners' equity—for comparative years. The independent auditor expresses an opinion on the fair presentation of financial statements in conformity with GAAP. The opinion can be one of four types:

1. *Unqualified (clean) opinion*. Financial statements present fairly, in all material respects, the company's financial position and results of operations in conformity with GAAP. This type of opinion can be given when the auditor has no reservations or qualifications about the reliability of the financial statements. This is the type of opinion an auditor likes to issue and clients prefer to receive; it means that all material financial disputes were resolved to the auditor's satisfaction prior to the issuance of the report.
2. *Qualified opinion*. The auditor's overall conclusion is positive regarding fair presentation of financial statements in conformity with GAAP except for one or more financial items or issues as explained in the explanatory paragraph of the report.
3. *Adverse opinion*. The opposite of the unqualified opinion. It means that the financial statements are not fairly presented in conformity with GAAP.
4. *Disclaimer of opinion*. This means that the independent auditor is issuing no opinion on the financial statements due to a lack of independence or inability to gather sufficient competent evidence.

The presence of financial statement fraud, in particular, warrants external auditors to modify their standard unqualified opinion. Failure of external auditors to detect financial statement fraud either because of negligent auditing or involvement in the fraud to protect their clients at the expense of investors can result in substantial losses to investors and creditors and lawsuits against auditors. The 1999 COSO report reveals that external auditors were named in more than 29 percent of the alleged fraud cases, and companies had changed auditors before detection of financial statement fraud in about 25 percent of cases.[4]

Arthur Andersen: The Demise of an American Legacy

Shining Days

The professional dilemma faced by Arthur Andersen in the chapter introduction was not unique; the Great Lakes steamship company was another challenge for the emerging firm. The decision hinged on the question of reflecting a loss in the current-period financial statements even though the loss did not occur until after the end of the period. In early February 1915, a steamship client lost a ship in a storm. The steamship company was preparing December 31, 1914, financial statements. Because it was planning to sell securities in 1915, the company did not want the loss disclosed in the December 1914 report, arguing that the loss did not occur until 1915. Arthur Andersen disagreed and

refused to issue the steamship company's financial statements without the disclosure. Today GAAP requires adequate recognition of impaired value; in 1915, however, Arthur Andersen was breaking new ground, a position founded on principle.

Arthur Andersen was a man of ideas and ideals.

Dark Days

On June 15, 2002, a jury found the accountancy firm of Arthur Andersen guilty of obstructing justice by shredding documents relating to the failed energy giant Enron. The verdict was the death knell for the 89-year-old company, one of the world's top five accounting firms at the time. The felony conviction prevented Andersen from signing public company audit reports to be filed with the SEC.

What Happened?

Arthur Andersen, who headed the firm until his death in 1947, was a zealous supporter of high standards in the accounting industry and a stickler for honesty, arguing that accountants' responsibility was to investors, not their clients' management. Yet in the late 1990s and early 2000s, the company was associated with a number of high-profile clients alleged to have committed financial statement fraud: Sunbeam Products, Qwest, Waste Management, Global Crossing, HBOCMcKesson, Asia Pulp and Paper, the Baptist Foundation of Arizona, WorldCom, and Enron.

Research suggests that Andersen made some bad choices; most describe the shortcomings as ethical lapses. Yet Kaplan, Roush, and Thorne cite three structural issues pervasive across the audit industry at the time:

1. Audit firm clients were under considerable pressure to produce financial information that met forecasts and market expectations.
2. Audit firms, not just Andersen, faced increased emphasis on growth. To motivate that growth, audit firm partners were compensated, at least in part, by their ability to attract new clients and retain old ones.
3. Clean peer review opinions among audit firms were common at the time.

Reputation Matters

While Andersen's problems were arguably associated with the choices made by a few individuals, and supported by a culture and climate that was very interested in profits and growth, outstanding and ethical Andersen professionals were devastated by the guilty verdict, both professionally and financially. We have observed similar outcomes in the demise of so many financial institutions related to the credit/mortgage subprime/unregulated derivative financial instruments crisis of 2008.

On May 31, 2005, the United States Supreme Court unanimously threw out the conviction of Arthur Andersen, a symbolic victory for the defunct professional services firm. The verdict reversal does little to restore the lives and livelihoods of those impacted; of course, the investors, creditors, and other stakeholders shattered by Andersen's choices were also left without much recourse.

Sources: See R. Duska, "The Good Auditor—Skeptic or Wealth Accumulator? Ethical Lessons Learned from the Arthur Andersen Debacle," *Journal of Business Ethics* 57 (2005). G. Staubus, "Ethical Failures in Corporate Financial Reporting," *Journal of Business Ethics* 57 (2005). Steven Kaplan, Pamela Roush, and Linda Thorne, "Andersen and the Market for Lemons in Audit Reports," *Journal of Business Ethics* 70 (2007).

INDEPENDENT AUDITOR AND FINANCIAL STATEMENT FRAUD

Financial statement fraud has been and continues to be a focus of the auditing profession. During the early 1990s, external auditors viewed the detection of fraud, particularly financial statement fraud, as the primary purpose of their financial audit. The auditing profession has moved from acceptance of fraud detection as a primary purpose to the expression of an opinion on fair presentation of financial statements during the twentieth century. Recently, the accounting profession has directly addressed the external auditor's responsibility for financial statement fraud detection in its Statement on Auditing Standards (SAS) No. 99 entitled *Consideration of Fraud in a Financial Statement Audit*.[5]

SAS No. 99 requires independent auditors to obtain information to identify financial statement fraud risks, assess risks by taking into account the entity's programs and controls, and respond to results of assessment by modifying audit plans and programs. SAS No. 99 also:

- Increases emphasis on professional skepticism by requiring members of the audit team exchange ideas or brainstorm how frauds could occur
- Requires discussions with management about its knowledge of fraud or suspected fraud, its awareness of any allegations of fraudulent financial reporting, its understanding about the risks of fraud in the entity, and the programs and controls it has established to mitigate specific fraud risk
- Requires discussions with management about the nature and extent of monitoring of operating locations or business segments and whether and how it communicates to employees its views on business practices and ethical behavior
- Requires auditors to make a point of talking to employees in and outside management in order to give employees and others the opportunity to blow the whistle
- Requires auditors perform unpredictable audit tests and respond to management override of controls

As depicted in Exhibit 11.2, in the corporate governance structure, the external auditor's role is to provide reasonable assurance regarding the quality, integrity, and reliability of the published, audited financial statements. Thus, the public expects auditors to detect financial statement fraud. In some instances, when auditors fail to detect financial statement fraud and it is discovered subsequent to their reports, the effectiveness of financial statement audit is questioned and the usefulness of the audit function is challenged. If audited financial statements are materially misleading and contain material frauds, and if investors and creditors use those statements for financial decision making, investors and creditors may allocate their resources uneconomically to unproductive companies. When auditors perform the audit with due diligence by observing generally accepted audit standards (GAAS), including

Exhibit 11.2 Corporate Governance and Its Functions

PCAOB auditing standards, and exercising due care, they have fulfilled their professional responsibility.

SAS No. 99 provides guidance on audit procedures to identify and examine related party transactions, especially when they contain red flags that indicate the likelihood of financial statement fraud. For example, when management intentionally fails to disclose material related party transactions or deliberately records them improperly, there is a higher probability that management also engaged in financial statement fraud. Although red flags do not always indicate financial statement fraud, they are present in many incidents of fraudulent financial reporting activities. It is the auditor's responsibility to assess the risk of fraud and plan and conduct an audit with relevant degrees of skepticism and professional judgment. Auditors cannot provide absolute assurance that they have detected fraud due to such factors as the existence of the employee fraud, a fraudulent transaction being immaterial, and imperfect in audit methods (e.g., using audit sampling testing). In identifying and assessing the risks of material financial statement fraud, auditors should:

- Make inquiries of audit committee and others charged with governance within the client organization to gather sufficient information about the risk of the fraud

- Communicate with the audit committee, management, and legal counsel about the allegations of fraud and how they are addressed
- Consider unusual, unexpected, or even unjustifiably normal evidence gathered through performing analytical procedures based on the business's financial condition and results
- Consider evidence gathered through the audit of internal control over financial reporting (ICFR) that may suggest the existence of one or more fraud risks factors and the fact that adequate and effective internal controls did not address the detected risk

Auditors should ask the audit committee, management, and others charged with corporate governance about the entity's antifraud policies and procedures and whether they are in writing, updated on a timely basis, implemented effectively, and enforced consistently. External auditors should not rely entirely on the work of internal auditors to identify fraud risk and audit procedures to test them. Internal auditors may provide limited direct assistance to external auditors in performing audit procedures to detect fraud. External auditors should pay attention to key performance indicators (KPIs), such as revenue measured per division or major customer, days sales outstanding, inventory turns, production utilization, profit margin, and others reported by their clients. Auditors should consider whether KPIs provide information consistent with the client's financial conditions and results of operation. Financial statement fraud often occurs when clients experience significant changes that affect their business operations and results. The most noticeable changes are often in the following:

- General or industry economic conditions
- Major customers or line of products
- Technology or product methods and processes
- Business strategy
- Management
- Regulatory environment affected by clients operations

Auditors should perform substantive tests to address the identified fraud risk.

A 2007 survey of 140 companies worldwide conducted by Ernst & Young shows that two-thirds of respondents reported their company had no formal fraud prevention program in place.[6] The wave of financial scandals of recent years has resulted in regulatory reforms to combat corporate malfeasance and for corporations to implement effective antifraud programs. Corporate gatekeepers (e.g., the board of directors, external auditors, legal counsel, etc.) have taken a proactive stand by asking management to present its antifraud program and by evaluating the risk that management may override internal controls. The existence of an antifraud program should be considered as an indicator of effective control to deal with

fraud. However, the absence of a formal antifraud program should not be interpreted as an organization's tolerance for fraud; other controls may prevent and detect fraud. The best antifraud program starts with a focus on a corporate culture of providing incentives and opportunities for doing the right thing and sets an appropriate tone at the top in promoting competent and ethical behavior. PCAOB's Auditing Standard No. 5 (AS5), *An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statement*,[7] is a fraud-focused standard that places increased emphasis on fraud risk, antifraud controls, and audit procedures to test the effectiveness of such controls in preventing and detecting financial statement fraud. Auditors are required to assess fraud risk in the audit of ICFR and factor into the assessment the extent, nature, and timing of substantive tests designed to discover financial statement fraud. The emphasis on identification and assessment of fraud risk and related controls is aligned with the SEC's Interpretive Guidance on management evaluation and assessment of ICFR,[8] which is expected to improve audit quality and promote the use of an integrated auditing.

INDEPENDENT AUDIT AND INTERNAL CONTROL

In the post-SOX period, regulators (SEC) and standard setters (PCAOB) have encouraged external auditors to integrate the audit of financial statements and internal controls. Auditors are encouraged not to waste their resources on testing low-level controls that are not significant; rather, they should focus on more important controls. An integrated audit requires auditors to change their audit strategy. Independent auditors traditionally have performed a combination of tests of controls and substantive tests to provide reasonable assurance that financial statements are free of material misstatements, whether caused by errors or fraud. This level of assurance requires auditors to reduce the risk of material misstatements to an appropriately low level. The level of tests of internal controls performed, including understanding of the client's internal control structure, is not sufficient to opine on internal controls. Tests of controls must be broadened to include understanding of ICFR and provide reasonable assurance about the effectiveness of both the design and the operation of internal controls. Prior to SOX, auditors traditionally performed limited tests of controls, used a cycle rotation approach to test controls, or conducted dual internal controls or substantive tests. These audit approaches are less relevant to an integrated audit.

AS5 provides guidance for auditors in making Section 404 audits more cost justified, efficient, and scalable. AS5 is intended to improve efficiency and effectiveness of audit of ICFR under Section 404 of SOX in seven ways:

1. Focusing audit attentions to the areas that pose the greatest risk that ICFR will fail to protect against material misstatements in the financial statements.

2. Using a principles-based, top-down approach that focuses on the importance of auditing higher-risk areas that can have a significant effect on ICFR (e.g., financial reporting closing process).
3. Encouraging auditors to consider a range of possible combinations of audit procedures in gathering sufficient and competent evidence needed according to the assessed level of risk.
4. Clarifying that an auditor is not required to evaluate management's assessment of the effectiveness of ICFR or opine on the adequacy of management's assessment process.
5. Clarifying the appropriate materiality standard to use in the audit of ICFR, which should be the same as materiality considerations applied in the audit of the company's annual financial statements.
6. Providing additional discussion of three broad categories of entity-level controls and how each category may have a different effect on the planning of the audit in the context of the selection and testing of other controls (e.g., entity-level controls that monitor the operation of other controls may reduce the need for testing the underlying and process-level controls).
7. Providing new definitions for *significant deficiencies* and *material weaknesses*.

The top-down, risk-based approach promoted in both the SEC's Interpretive Guidance and AS5 is designed to refocus both management and auditors on controls that matter and risks that threaten the integrity and reliability of financial reports. Both AS5 and the SEC's Interpretive Guidance are intended to bring down the compliance costs of Section 404.

REPORT ON INTERNAL CONTROLS

The independent audit report on ICFR can be a separate report or combined with the audit report on financial statements. Exhibit 11.3 shows the format and content of a combined report of both a financial statement audit and an internal control audit according to AS5. It is expected that the auditing profession will eventually move toward an integrated audit approach (the combined audit of both ICFR and financial statements), which will necessitate the use of an integrated audit report. An integrated audit report should be issued particularly when the independent auditor issues an unqualified opinion on both financial statements and ICFR. Nevertheless, management's report on internal control should be a separate report and should be placed right after the management's discussion and analysis (MD&A) section of Form 10-K and immediately before the financial statements section.

The independent auditor should issue an opinion on ICFR, either as a separate report or as a combined report with an opinion on the financial statements. If the auditor chooses to issue a separate report on ICFR, he or she should add a paragraph specifying that ICFR is being audited, and the report date should be the

Exhibit 11.3 Report of Independent Registered Public Accounting Firms

[*Definition paragraph*]

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of recrods that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

[*Inherent limitation paragraph*]

Because of inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

[*Opinion paragraph*]

In our opinion, management's assessment that W Company maintained effective internal control over financial reporting as of December 31, 20X3, is fairly stated, in all material respects, based on [*Identity control criteria, for example, ''criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).'']*. Also in our opinion, W Company maintained, in all material respects, effective internal control over financial reporting as of December 31, 20X3, based on [*Identity control criteria, for example, ''criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission(COSO).''*].

[*Explanatory paragraph*]

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the [*identify financial statements*] of W Company and our report dated [*date of report, which should be the same as the date of the report on the effectiveness of internal control over financial reporting*] expressed [*include nature of opinion*].

[*Signature*]

[*City and State of Country*]

[*Date*]

Source: Adapted from the Public Company Accounting Oversight Board; available at www.pcaobus.org.

same as the date of report on the financial statements. The six key elements of both a separate report and a combined report are:

1. A statement that management is responsible for maintaining effective ICFR and for assessing the effectiveness of ICFR
2. A statement that the auditor's responsibility is to express an opinion on the company's ICFR
3. A definition of ICFR
4. A statement that the new audit was conducted in accordance with the standards of the PCAOB
5. A statement regarding the limitations of ICFR
6. The auditor's opinion on whether the company maintained, in all material respects, effective ICFR based on the control criteria as of the specified date.

There are three possible types of audit opinions on ICFR:

1. *Unqualified opinion*. The unqualified opinion can be rendered when there are no identified material weaknesses in ICFR and no scope limitations. In this case, the audit report states: ''In our opinion, the company's internal control over financial reporting is effective.''
2. *Adverse opinion*. The adverse opinion should be rendered when there are significant deficiencies in the company's ICFR that result in one or more material weaknesses. In this case, the audit report states: ''In our opinion, the company's internal control over financial reporting is ineffective.''
3. *Qualified/disclaimer opinion*. The disclaimer opinion should be given when there is a scope limitation and the auditor cannot express an opinion on management's assessment of the effectiveness of the company's ICFR.

FRAUD DETECTION AUDIT PROCEDURES

A broad variety of audit procedures can be used to detect financial statement fraud. SAS Nos. 99 and PCAOB auditing standards provide guidance regarding the auditor's response to the results of risk assessment by making judgments about the risk of material financial statement fraud. This risk assessment affects the audit in a number of ways.

PROFESSIONAL SKEPTICISM

Due professional care requires external auditors to exercise professional skepticism, which is an attitude that includes a questioning mind and a critical assessment of auditor evidence. Two examples of the application of professional skepticism in assessing the risk of material financial statement fraud are:

1. Increased sensitivity and due professional care in selecting the nature, timing, and extent of audit procedures in gathering sufficient audit evidence to substantiate material transactions and account balances
2. Increased recognition of the need to corroborate management assertions and representations regarding material financial items and matters by performing thorough analytical procedures, examining documents, and discussing with others within and/or outside the client's company

ASSIGNMENT OF PERSONNEL

The results of risk assessment may indicate the possibility of financial statement fraud, which necessitates the assignment of knowledgeable, skilled, and well-trained auditors and specialists to improve the likelihood of fraud detection. Furthermore, the quality and extent of supervision should recognize the risk of material misstatement caused by financial statement fraud and the qualifications of auditors performing supervision.

ACCOUNTING PRINCIPLES, POLICIES, AND PRACTICES

The possibility of financial statement fraud requires auditors to pay special attention to management's selection and application of significant accounting policies regarding revenue recognition, asset valuation, and capitalization versus expensing major expenditures. The 1999 COSO report indicates that more than half of the SEC enforcement actions regarding financial statement fraud relate to improper revenue recognition.[9] Auditors should satisfy themselves that the selected accounting principles are appropriate and that applied accounting policies are consistent and acceptable.

INTERNAL CONTROLS

When the results of risk assessment indicate the likelihood of financial statement fraud, auditors should ensure that the internal control system is adequate and effective in preventing, detecting, and correcting such fraud. When the internal control risk is considered to be high, indicating the failure of internal controls to prevent and detect risk, auditors should rely on their own test procedures to detect financial statement fraud. The degree of internal control risk would determine the extent, timing, and nature of audit procedures performed to discover financial statement fraud.

EFFECT OF FRAUD RISK FACTORS ON AUDIT PROCEDURES

The extent, timing, and nature of audit procedures should be modified when risk factors indicate the likelihood of financial statement fraud. Auditors should take these three steps:

1. They should change the nature of audit procedures in order to obtain audit evidence that is more reliable, relevant, and pervasive, and gathered from independent sources outside the company.
2. They may need to change the timing of audit procedures to be closer to or at year-end. When there are motivations and opportunities for management to engage in financial statement fraud, auditors should perform their audit procedures near or at the end of the reporting period to detect misstatements and assess their impacts on the integrity, quality, and reliability of financial statements.
3. They must consider the likelihood of financial statement fraud when determining the extent of audit procedures to be applied. Auditors should enlarge the sample size to factor in the additional risk and to ensure that the selected sample will discover suspected financial statement fraud. The audit should focus specific attention on areas in which the likelihood of fraud occurrence is higher, particularly revenue recognition, accounts receivable, inventories, liabilities, and fixed assets. Thus, auditors should gather persuasive evidence to determine whether material financial statement fraud has occurred or is likely to have occurred. If it has, auditors should determine its impact on fair presentation of financial statements and their report.

Auditors are required to plan and perform an audit in accordance with PCAOB auditing standards to provide reasonable assurance that the financial statements are free of material misstatements caused by errors and frauds. Material misstatements often include overstatements of revenues and assets and understatements of expenses and liabilities. Although management is more prone to overstate revenues and understate expenses to meet analysts' earnings forecasts, auditors should pay attention to both understatements and overstatements of revenues, expenses, assets, and liabilities. Any misstatements of financial transactions or account balances will cause financial statement fraud. SAS No. 99 also identifies specific approaches that may be used when it is likely that financial statement fraud has occurred. The suggested audit approaches, among others, include:

- Performing certain audit procedures (e.g., analytical procedures, substantive tests)
- Changing the audit approach in the current year
- Counting inventories at a date closer to year-end
- Investigating the possibility of related party transactions
- Performing a thorough review of quarter-end and/or year-end closing entries and further investigation of any unusual closing transaction entries
- Conducting detailed interviews of personnel involved in areas indicating the likelihood of financial statement fraud
- Using the work of specialists when expertise in understanding and detecting the nature and amounts of financial statement fraud is needed

FORENSIC FIELD AUDIT

External auditors are in a position to detect financial statement fraud and prevent further occurrence of the same fraud. The O'Malley Panel on Audit Effectiveness[10] recommends that external auditors use forensic-type fieldwork audit procedures by using a high level of professional skepticism throughout the audit process and paying special attention to fraud symptoms and red flags that may signal financial statement fraud. Auditors should use forensic-type fieldwork audit procedures and continuous transaction testing in areas particularly susceptible to fraud. In compliance with current GAAS, auditors should employ the audit risk model, which encourages auditors to use judgment in assessing audit risk and in selecting risk-based audit procedures based on the individual client company's nature, condition, and circumstances. This risk-based audit approach of continuous testing of high-risk areas can contribute to audit efficiency and effectiveness in detecting financial statement fraud.

To protect investors and creditors and safeguard them from receiving fraudulent and misleading financial information, auditors should:

- Ensure that their audit strategy is appropriate in the circumstance
- Assess and document the client's internal control environment, including management's philosophy and operating style
- Conduct appropriate audit procedures in gathering sufficient and competent evidence on the substance rather than the form of the client's policies and procedures

The use of a risk-based audit approach requires auditors to become familiar with their client's business, industry, and operating strategies; however, auditors' close involvement in the daily operation activities and management functions of the client can cause their independence to be questioned or even impaired. For example, the auditor's involvement and direct participation in determining earnings forecasts for the client may create the appearance that the auditor is verifying the accuracy or achievability of the earnings forecast—a situation that, in turn, may diminish the auditor's objectivity and independence.

When Auditors Succeed

When auditors fail, the announcement often makes the headlines, but how about when auditors succeed? According to the Association of Certified Fraud Examiners (ACFE) *Report to the Nation*, external auditors discover the fraud about 10 percent of the time. Further, external auditors identify over 14 percent of frauds discovered in small businesses and in almost 15 percent of the cases are responsible for detecting fraud in not-for-profit organizations. The reality is that every day auditors discover and help their clients resolve

(*continued*)

deficiencies, irregularities, exceptions, anomalies, and fraud. Given the materiality threshold used by external auditors, they are not expected to detect every fraud. More important, discovered fraud often goes unreported and is quietly resolved behind closed doors. And so, for auditors, the ultimate measure of success is not fame and fortune but moral character and personal integrity.

Since the passage of SOX, external auditors have felt more empowered. According to numbers reported in the *CPA Journal* (Owens-Jackson, Lisa, Diana Robinson, and Sandra Shelton, "Auditor Resignations and Dismissals," *CPA Journal*, January 2008), auditor resignations grew significantly in the post-SOX time frame, increasing from 89 (0.7 percent of audits) in 2001 to a high of 139 (1.5 percent of clients) in 2004. Auditors have more quickly ended their relationship with difficult clients and have been less willing to accept integrity risk. Interestingly, Big Four audit firm dismissals are also up, but those increases are believed to be associated with increases in audit fees.

So what are auditors to do when they discover a difficult situation that cannot be resolved with their client, where the evidence might heighten suspicion but not clearly indicate material misstatement or fraud? According to the AICPA ethics rules on integrity and objectivity, auditors should not subordinate their judgment to others. According to AICPA Professional Code of conduct Rule 102, if a member and his or her supervisor have a disagreement or dispute relating to the preparation of financial statements or the recording of transactions, the member should take these steps:

1. The auditor should consider whether (a) the entry or the failure to record a transaction in the records, or (b) the financial statement presentation or the nature or omission of disclosure in the financial statements, as proposed, represents the use of an acceptable alternative and does not materially misrepresent the facts. If the matter has authoritative support and/or does not result in a material misrepresentation, the member need do nothing further.
2. If the auditor concludes that the financial statements or records could be materially misstated, the auditor should make his or her concerns known to the appropriate higher level(s) of management within the organization (e.g., the supervisor's immediate superior, senior management, the audit committee or equivalent, the board of directors, the company's owners).
3. If, after discussing his or her concerns with the appropriate person(s) in the organization, the auditor concludes that appropriate action was not taken, he or she should consider his or her continuing relationship with the employer. The auditor also should consider any responsibility that may exist to communicate to third parties, such as regulatory authorities. In this connection, the auditor may wish to consult with his or her legal counsel.
4. Nonauditors should be cognizant of the obligation to be candid with external accountant and not knowingly misinterpret facts or fail to disclose material facts to him or her.

Sources: ACFE, *Report to the Nation on Occupational Fraud and Abuse*, 2008. Lisa Owens-Jackson, Diana Robinson and Sandra Shelton, "Auditor Resignations and Dismissals," *CPA Journal* (January 2008). AICPA Professional Code of Conduct Rule 102.

FRAUD AUDITING

SAS No. 99 was issued in 2002. Although it did not increase an independent auditor's responsibility for detecting fraud, it provided guidelines on how the auditor should respond when an assessment indicates a heightened risk of material misstatements of the financial statements because of fraud. This statement:

- Describes the process of conducting the risk assessment
- Includes a comprehensive listing of risk factors that an auditor should consider in the risk assessment
- Provides specific guidance in responding to the results of the risk assessment and documentation of the auditor's risk assessment and response
- Offers guidelines in evaluating the results of an audit test and communicating evidence of fraud to management, the audit committee, or others (e.g., SEC, regulatory bodies) as appropriate

FRAUD RISK FACTORS

SAS No. 99 identifies categories of risk factors (red flags) mostly related to financial statement fraud and two classes of red flags pertaining to misappropriation of assets. Financial statement fraud red flag categories are those associated with three areas:

1. Management's characteristics and influence over the control environment
2. Industry conditions
3. Operating characteristics and financial stability

The two red flags pertaining to misappropriation of assets are:

1. Susceptibility of assets to misappropriation
2. Controls

SAS No. 82 identifies more than 50 risk factors (red flags) related to financial statement fraud and misappropriation of assets. Auditors are required to document the existence of these risk factors and audit considerations and responses to those risk factors either individually or collectively.

SAS No. 99 requires external auditors to consider risk factors as red flags, warning signals, or symptoms that fraud may exist. These risk factors, individually or collectively, may be symptoms of possible financial statement fraud:

- Substantial related party transactions outside the ordinary course of business or with unaudited entities

- Material, unusual, or highly complex transactions, especially those close to the end of a reporting period
- Substantial operations or bank accounts in tax havens for which there is no legitimate business justification
- An organizational structure with a huge degree of unwarranted complexity

MATERIALITY GUIDANCE

Auditors often have to use their judgment to decide whether an error or misstatement is material enough to influence the decision-making process of investors and creditors. In fact, an auditor's opinion is formed based on the concepts of materiality and audit risk. Auditors, in their audit reports, state whether financial statements fairly present, *in all material respects*, the financial position, results of operations, and cash flows in conformity with GAAP. Thus, sound materiality judgments are important contributory factors in maintaining investor and creditor confidence in the financial reporting process. In making material judgments, auditors consider both qualitative factors (e.g., nature of an item, circumstances) and quantitative factors (e.g., absolute size, relative size, cumulative effects).

Materiality is defined in Statement of Financial Accounting Concept No. 2 as:

> The magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement.[11]

Audit risk is defined as the risk of issuing an inappropriate audit opinion (e.g., the risk of issuing an unqualified opinion on *materially* misstated financial statements or the risk of issuing an opinion other than unqualified on *materially* stated financial statements). Thus, audit risk is defined in the context of materiality. Auditors use materiality judgments in all stages of an audit process, from the planning phase of the audit to the final reporting stage. Auditing standards require auditors to use both qualitative and quantitative factors in assessing materiality. Twelve qualitative factors often used by auditors in making materiality judgments are:

1. Possible impact of misstatement on projected earnings
2. Likelihood of earnings management
3. Existence of restrictive debt covenants
4. Possible impact of misstatement on share price
5. Likelihood of financial statement fraud
6. Potential business combinations (e.g., mergers, acquisitions)
7. Imminent public stock offering

8. Detection of fraud or fraud symptoms in prior periods
9. Risk of litigation
10. Inadequate and ineffective internal control structure
11. Nonexistence of ineffective audit committee
12. Lack of vigilant board of directors

Examples of quantitative factors are absolute size of misstatements, cumulative size, and the amount of misstatements as a percentage of total assets or net income. Auditors, in assessing materiality, should pay special attention to the sensitivity of the capital markets to price-earnings multiples, especially when even a penny-a-share difference between the reported earnings and analysts' forecasted earnings is likely to trigger an investor response that could adversely affect market capitalization by millions of dollars. To assist auditors in making appropriate materiality judgments, the SEC, in its Staff Accounting Bulletin (SAB) No. 99, issued in September 2006,[12] discusses quantitative factors to consider in assessing materiality and encouraging registrants to record proposed audit adjustments.

SAB No. 108 addresses diversity in practice in quantifying materiality concerning financial statement misstatements and the potential problems under such practice for the proper financial statements. The bulletin provides interpretive guidance on how public companies should quantify financial statement misstatements and identifies two methods commonly used to accumulate and quantify misstatements: the rollover and iron curtain approaches. Under the rollover approach, a misstatement is quantified based on the amount of the error occurring in the current-year income statement, regardless of the carryover effects of prior-year misstatements. By focusing primarily on the income statement effects of misstatements, this approach can result in the accumulation of material misstatements on the balance sheet that are considered immaterial, primarily because the amount that originates in each year is quantitatively small.

By focusing primarily on the balance sheet effect of misstatements, the iron curtain approach quantifies a misstatement based on the effects of correcting the error as of the current-year balance sheet date, regardless of the year(s) in which the misstatement originated. The primary shortcoming of this approach is its failure to consider the correction of prior-year misstatements in the current year as errors. Thus, neither the rollover approach nor the iron curtain approach properly quantifies all misstatements that could be material to users of financial statements. SAB No. 108 suggests the use of an integrated approach (a combination of both the rollover and iron curtain approaches), which provides a more appropriate quantification of materiality assessment for the discovery of misstatements, including both the carryover and reversing effects of the prior- and current-year misstatements. SAB No. 108 is effective for the fiscal year ending after November 15, 2006, and thus for many public companies' 2006 annual financial statements of calendar year-end. The bulletin also provides transition accounting and disclosure guidance where the application of the dual approach (rollover and iron curtain) may result in

a material misstatement in the prior-period financial statements. In compliance with SAB No. 108, companies are allowed to restate prior-period financial statements or recognize the cumulative impact of restatements through an adjustment to beginning retained earnings in the year of adoption. Nonetheless, the Committee on Capital Markets Regulation urges the SEC to establish rules and interpretations to raise the threshold of materiality required to make a misstatement significant to the level that it would be subject to litigation.[13] A more reasonable materiality standard should be established for both internal controls and financial statements.

Auditors should use four steps in assessing and applying materiality under an integrated audit approach:

1. Define materiality as the largest amount of misstatement in the financial statements that could exist and still not affect the decisions of reasonable users and thus not cause auditors to qualify their opinion on the statements. Traditionally, auditors have used a percentage of income or other financial items (net assets) to determine overall materiality. Auditors should use both qualitative factors (i.e., trend in earnings, nature, circumstances) and quantitative factors (e.g., 5 percent of net income) to establish planning materiality.
2. Allocate the overall materiality to individual financial items or classes of transactions and related management assertions. This allocation is necessary because auditors typically perform tests of controls and substantive tests on transaction cycles and related accounts and classes of transactions. Auditors often use quantitative analysis to allocate the planned overall materiality to balance sheet accounts. The allocated materiality to the individual account balance is commonly referred to as tolerable misstatement. It determines the maximum amount of misstatement that could exist in the account while the auditor still decides that the account is fairly stated.
3. Decide on the materiality of the detected misstatements or internal control deficiencies. If the detected misstatement is considered to be material, the auditor should ask management to correct it. If the misstatement is regarded as immaterial, it can be waived. Auditors also use the concept of materiality in deciding whether the discovered internal control deficiencies are significant deficiencies that should be reported to the audit committee or material weaknesses that should be disclosed in the audit report on ICFR.
4. Apply authoritative guidance (e.g., SAB No. 108) in making a materiality judgment. Whenever an error is identified in the financial statements or a weakness is discovered in internal controls, auditors should assess whether the identified misstatement or weakness is material to the quality of financial statements or the effectiveness of internal controls. Auditors usually consider materiality from both qualitative and quantitative perspectives. Materiality is a matter of professional judgment, and its analysis requires the proper use of professional judgment. Nevertheless, the starting point is to quantify the amount of the misstatement by using either the rollover or iron curtain approach, or a combination of these

methods. In the post-SOX era, independent auditors should use the guidance provided in SAB No. 108 to quantify the misstatement and assess its materiality.

Satyam Fraud Creates Challenges for Auditing Profession

With 53,000 employees, Satyam Computer Services LTD is one of India's largest outsourcing companies, claiming to service one-third of Fortune 500 companies. In early January 2009, founder and CEO Ramalinga Raju wrote a letter to the Satyam board of directors, outlining a massive fraud; in the letter, Raju cited his own role in the perpetration and concealment of the fraud.

Satyam is a major corporation, audited by an Indian affiliate of a U.S.-based Big Four accounting firm. Because Saytam provides outsourcing services, the fraud has a unique twist: When companies outsource material operations to vendors, according to AICPA Statement on Auditing Standards (SAS) No. 70, company auditors rely on reports prepared by the vendors' auditors in order to attest to the financial controls over the outsourced operations. Shaalu Mehra suggests that the apparent failure of Satyam's internal controls may raise uncertainty regarding continued reliance on such reports, and outsourcing customers may seek further guidance from the SEC. It remains to be seen if these developments will, in the longer term, trigger a reassessment of the SAS No. 70 standard by the PCAOB and/or SEC.

Sources: AICPA Statement on Auditing Standards (SAS) No. 70. Shaalu Mehra, "Opinion: The Satyam fraud has important ramifications for outsourcers," *Computer World*, January 12, 2009.

RISK FACTORS OF FINANCIAL STATEMENT FRAUD

The audit risk model is an appropriate approach to justifying the method of gathering the audit evidence; however, any time the element of "judgment" is introduced into audit planning, different amounts of audit evidence-gathering procedures can be applied. The audit risk model is not intended to be a mathematical model. Certain minimum standards should apply in all situations. The specification of risk model is different under an integrated audit approach. Auditors use the audit risk model to justify the means of gathering evidence through performing both controls and substantive tests. In the auditing literature and authoritative statements, the audit risk model is specified in this way:

$$AR = IR \times CR \times DR$$

where

AR = audit risk
IR = inherent risk
CR = control risk
DR = detection risk

Audit risk is the risk that the auditor will issue an inappropriate audit opinion or will fail to modify the opinion on materially misstated financial statements, for example, issuing an unqualified opinion on such statements. *AR* in practice often has been quantified as 1 minus reasonable assurance. For example, if reasonable assurance provided by the independent auditors on the financial statements is 90 percent, the audit risk would be 10 percent.

Inherent risk is the risk of the susceptibility of an assertion to material misstatements in the absence of proper internal controls. It is the risk that material misstatements will enter into the financial reporting process because of ineffective corporate governance, lack of management integrity, or relative risk relevant to individual accounts. Management is primarily responsible for managing and controlling the inherent risk; the auditor's responsibility is to assess this risk and its impact on the audit plan.

Control risk is the risk that internal controls will fail to prevent, detect, or correct material misstatements that could occur in an assertion or enter into the financial reporting process. Management is responsible for establishing and maintaining an adequate and effective internal control structure to prevent errors, irregularities, and fraud on a timely basis. The auditor's responsibility is to assess the control risk and determine its impact on audit planning of internal control over both financial reporting and financial statements.

Detection risk is the risk that audit procedures will fail to discover material misstatements, given that they have entered into the financial reporting process and went undetected by the internal control structure. The auditor is primarily responsible to manage and control the detection risk by designing and implementing an effective audit strategy. Detection risk can be classified into analytical procedures risk, which is the risk that analytical procedures will fail to detect material misstatements, and substantive tests of details risk, which is the risk that substantive tests will fail to detect material misstatements that are not detected by internal controls and analytical procedures. This audit risk model should be used under the integrated audit approach to determine the timing, nature, and extent of both tests of controls and substantive tests.

In 2006, the AICPA issued eight new risk assessment standards (SAS Nos. 104–111).[14] These standards provide guidance for auditors to apply the audit risk model and form an opinion on client financial statements, including:

- Assessing audit risk
- Assessing materiality and tolerable misstatement
- Financial statement assertions
- Risk assessment procedures
- Understanding the entity, its environment, and internal control
- Assessing the risk of material misstatement

- Designing and performing appropriate audit procedures that effectively respond to the assessed risks
- Evaluating misstatements

SAS No. 99[15] indicates that risk factors that relate to financial statement fraud can be grouped into three categories: (1) management's characteristics and influence over the control environment, (2) industry conditions, and (3) operating characteristics and financial stability.

RISK FACTORS PERTAINING TO MANAGEMENT'S CHARACTERISTICS

Risk factors pertaining to management's characteristics and influence over the control environment are aimed at identifying pressure or an incentive to engage in financial statement fraud and perceived opportunity to commit such fraud. The risk factors involving management's motivations to engage in financial statement fraud are listed next.

- A considerable portion of management's compensation, represented by bonuses, stock options, or other incentives, pressure management to achieve unduly aggressive targets for operating results, financial position, or cash flow
- Commitments to analysts or creditors for unduly aggressive or unrealistic forecasts
- Undue pressure on management and/or interest by management in maintaining or increasing the company's stock price or earnings trend through the use of unusually aggressive accounting practices (e.g., earnings management)
- The use of inappropriate means to minimize earnings for tax-motivated purposes
- Domination of management by a single person or small group without effective monitoring oversight by the board of directors and/or the audit committee
- Ineffective communication and support of entity values and ethics
- Management failure to correct known reportable conditions
- Management disregard for regulatory authorities
- Management setting unduly aggressive financial targets and expectations for operating personnel
- High turnover of senior management, counsel, or board members
- Management continuing to employ ineffective and incompetent accounting, information technology, or internal audit staff
- Unreasonable demands for auditor completion of the audit or report issuance
- Formal or informal restrictions on auditor access to people or information

- Domineering management behavior or attempts to influence audit scope
- Known history of securities law violations or fraud or allegations of financial statement fraud

RISK FACTORS RELATING TO INDUSTRY CONDITIONS

Risk factors relating to industry conditions, such as a high degree of competition or market saturation, accompanied by declining margins and unduly aggressive performance measures, can pressure management to improve operating results, financial position, and cash flows. Examples of these risk factors, specified in SAS No. 99, are (1) new accounting, statutory, or regulatory requirements that could impair profitability or financial stability and (2) extensive market competition or saturation, accompanied by declining margins.

RISK FACTORS RELATED TO OPERATING CHARACTERISTICS AND FINANCIAL STABILITY

Factors relating to operating characteristics and financial stability, such as unrealistically aggressive sales or profitability incentive programs, can pressure management and personnel to engage in fraudulent financial activities. Examples of these factors are the following:

- An inability to generate operating cash while reporting earnings growth
- Significant, unusual, or highly complex transactions, especially near year-end, that pose "substance over form" questions
- Bank accounts or operations in tax-haven locations without clear business purpose
- Unusually rapid growth or profitability compared to others in the industry
- A threat of imminent bankruptcy or hostile takeover
- A poor or worsening financial position when management has personally guaranteed significant entity debt

SAS No. 99 requires a specific fraud risk assessment in every audit engagement. Auditors must ask management about areas of potential fraud risk and how it is managing these risks or intends to address such risks.

DOCUMENTATION OF RISK FACTORS

Financial statement fraud is a sensitive issue that requires effective and proper documentation at every stage of the audit process. In the audit planning stages, auditors should manually or electronically document in the working papers evidence that they have performed an assessment of the risk factors pertaining to financial

statement fraud. Auditors also should document how they address and respond to fraud risk factors. During the performance of the audit, if auditors identify any risk factors or other condition that lead to reassessing fraud risk, they should make the proper documentation describing their response to those risk factors. SAS No. 99 gives auditors flexibility in deciding how to document identified risk factors, their responses to the risk factors, actions they have taken, and communication issues related to fraud. Auditors may include the underlying rationale behind the selected risk factors and/or an explanation of their assessed level of fraud risk and any fraud-related inquiries.

COMMUNICATION OF FRAUD

Once auditors have discovered a fraud or a possible fraud, all evidence regarding the fraud should be reviewed and verified, and legal counsel should be contacted if auditors deem it necessary; however, the communication should be limited to those who need to know. Such communication may involve senior management, the audit committee, the board of directors, and, when appropriate, others outside the client's organization. Top-level management typically is involved in financial statement fraud. In this case, auditors should report the discovered financial statement fraud directly to the audit committee or, in its absence, to the board of directors. If the auditors determine that identified fraud risk factors have continuing internal control implications, they should consider including those risk factors in the required communication of reportable conditions to senior management and the audit committee.

The disclosure of financial statement fraud to parties outside of the client's organization is ordinarily precluded and prevented by auditors' ethical and legal obligations of conditionality, unless the matter is reflected in the auditors' report; however, auditors should recognize that, in the case of financial statement fraud, and in the next four circumstances, a duty to disclose fraud outside the entity may exist:

1. To comply with certain legal and regulatory requirements
2. To a successor auditor when the successor auditor makes inquiries in accordance with SAS No. 84, *Communications between Predecessor and Successor Auditors*[16]
3. In response to a subpoena in light of the concept that gathered audit evidence is not privileged and thus cannot be withheld from a court of law (e.g., AICPA trial board, SEC lawsuit cases)
4. To a funding agency or other specified agency in accordance with requirements for the audits of entities that relieve governmental financial assistance

The Private Securities Litigation Reform Act (PSLRA) of 1995 applies to publicly traded companies covered by the 1934 Securities Act and requires auditors to report discovered financial statement fraud.[17] Section 10a(b)of the act requires

auditors to provide the SEC with notification of material illegal acts, including financial statement fraud that has not been responded to in a timely manner by senior management, has been communicated to the audit committee, has been brought to the attention of the board of directors, and has not been reported to the SEC by the board. The PSLRA has effectively created a whistle-blowing obligation for auditors of publicly traded companies. The SEC position has been that illegal acts described in the PSLRA relate to financial statement fraud, not to the illegal acts by the client's managers and employees that do not have a direct and material effect on the presentation of financial statements. When the outsider determines that an illegal act has a material effect on the financial statements (e.g., financial statement fraud) but senior management has not taken the appropriate remedial action, either on its own or at the demand of the board of directors, the auditor should communicate that matter to the audit committee and issue a formal report to the board. The board of directors has only one business day to notify the SEC and the auditor of its compliance with notifying the SEC.

Under the PSLRA, auditors are obligated to report to the SEC that they have detected financial statement fraud and management will not remedy the situation by restating the financial statements or reporting financial statement fraud to the SEC. Auditor notification is required even if the auditor decides to resign from the engagement. Failure of the auditor to comply with the required notices may make him or her subject to civil penalties under the 1934 Securities Act.

ANTIFRAUD APPLICATIONS FOR PRACTICE

One reason why auditors are a deterrent is because most perpetrators fear getting caught and the associated consequences. Of course, auditors increase the perception of detection as well as the likelihood of catching fraudsters. Professionals can use the next information in their interactions with auditors to ensure that the auditors' efforts with regard to fraud detection will help reduce the risk of undetected fraud.

To enhance the perception of detection, audits are designed to:

- Occur as part of ordinary operations
- Draw on external sources of information (''financial fingerprints'' left at banks, with vendors and customers)
- Include a process to alert appropriate persons when issues, deficiencies, irregularities, exceptions, and anomalies are observed
- Include a process to resolve issues, deficiencies, irregularities, exceptions, and anomalies in an ethical and professionally competent manner

Auditors should include an examination of whistle-blower hotlines and other reporting mechanisms:

- For public companies regulated by SOX, a hotline or a similar reporting mechanism is required.
- The ACFE notes that tips and accidental discovery are the primary means by which fraud is discovered.
- The hotline mechanism should be multilingual, have 24/7 availability, include genuine anonymity, ensure no retaliation or retribution against persons who reports concerns, and ensure appropriate and timely reaction to the concerns of those reporting.
- Hotline existence and availability should be communicated to employees, customers, vendors, and suppliers.
- Hotline personnel need to have a protocol for whom to notified depending on the type of information received: manager/supervisor, senior management, audit committee, legal, human resources, ethics/compliance officer, security.
- The hotline should be tested periodically by internal audit.

In their audit procedures with respect to fraud, auditors should examine traditional internal controls that mitigate the risk of fraud, including reconciliations, independent internal reviews, and appropriate approvals. They should conduct independent physical inspections, periodic inventory counts, confirmations with outside transaction participants, performance analysis, and compliance testing. External audit procedures, like those of internal auditors, should be unpredictable.

Considering the risk of epidemics of fraud, external audit procedures should include an assessment of emerging industry practices as well as fraud and the likelihood that those activities will manifest in the entity under examination.

External auditors should incorporate proactive fraud detection procedures in areas with high probabilities of fraud occurrence and significant dollar magnitude, including data analysis, continuous auditing and the investigation of anomalies (e.g., red flags), unexpected trends, suspicious journal entries (reversing journal entries; journal entries to increase revenues or decrease expenses), Benford's law violations (using the Benford's Law, one can form expectations about the frequencies of tabulated numbers and any deviations from such expectations can be investigated using appropriate procedures), and data mining. Data extraction and analysis, also called data mining, can be used proactively for these purposes:

- Identify unknown, hidden relationships
- Identify suspicious transactions
- Assess the effectiveness of internal controls (compliance)
- Monitor threats and unmitigated fraud risks
- Examine and analyze "mountains" of data effectively and efficiently

Proactive fraud detection also includes an active search for collusion and management override:

- Review of journal entries
- Review of estimates
- Review of unusual/significant (nonrecurring) transactions

Electronic discovery (also called e-discovery) refers to any process in which electronic data are sought, located, secured, and searched with the intent of using the data as evidence in a civil or criminal legal case. Although not currently used in audits, e-mail and electronic communications—captured and available for legal reasons—may someday be available for audit examination. The inclusion of e-mail and electronic communications as audit evidence is clearly controversial, but the rewards to auditors could be significant.

Auditors may derive benefits from reviewing management's documentation of written detection protocols with respect to fraud prevention, deterrence, and detection:

- Overall fraud detection process
- Specific fraud detection controls
- Implementation of those controls
- How management monitors the existence and effectiveness of detection controls
- How management approaches continuous improvement: assessing and updating the design and implementation of deterrence and detection tools and techniques

Auditors may also want to examine client management reports of the performance of antifraud efforts, paying particular attention to:

- Recurring frauds
- Losses and the value associated with preventing future (similar) frauds
- The timeliness of design changes/improvements in fraud prevention, deterrence, and detection activities

Last thought:

> *Associate with men of good quality if you esteem your own reputation; for it is better to be alone than in bad company.*
>
> —George Washington

NOTES

1. *Arthur Andersen & Co.: The First Fifty Years (1913–1963)* (Chicago: Arthur Andersen and Company, 1963).

2. U.S. Chamber of Commerce, *Auditing: A Profession at Risk* (January 2006); available at www.uschamber.com.
3. American Institute of Certified Public Accountants, *Statement on Auditing Standards No. 99: Consideration of Fraud in a Financial Statement Audit*, 2002; available at www.aicpa.org/download/auditstd/summarysas99.doc.
4. Zabihollah Rezaee, *Corporate Governance Post-Sarbanes Oxley: Regulations, Requirements and Integrated Processes* (Hoboken, NJ: John Wiley & Sons, 2007).
5. American Institute of Certified Public Accountants, *Consideration of Fraud in a Financial Statement Audit. SAS No. 82* (New York: Author, 1997).
6. Ernst & Young, ''From Compliance to Competitive Edge: New Thinking on Internal Control'' (May 2007); available at www.ey.com/Publication/vwLUAssets/AABS_RAS_-_Internal_Controls_From_Compliance_to_Competitive_Edge/$FILE/AABS_RAS_Internal_Controls_From_Compliance_to_Competitive_Edge.pdf.
7. PCAOB, Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting that Is Integrated with an Audit of Financial Statements*, May 24, 2007; available at pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf.
8. SEC 17 CFR part 241, Commission Guidance Regarding Management's Report on Internal Control over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, June 27, 2007; available at www.sec.gov/rules/interp/2007/33-8810.pdf.
9. M. S. Beasley, J. V. Carcello, and D. R. Hermanson, *Fraudulent Financial Reporting: 1987–1997, An Analysis of U.S. Public Companies* (New York: COSO, 1999).
10. The Panel on Audit Effectiveness. Reports and Recommendations, August 31, 2000; available at www.pobauditpanel.org/downloads/prefatory.pdf.
11. Financial Accounting Standards Board, *Statement of Financial Accounting Concepts No. 2. Quantitative Characteristics of Accounting Information* (May 1980); available at www.fasb.org/st.
12. Securities and Exchange Commission, *Staff Accounting Bulletin No. 108*, September 13, 2006; available at www.sec.gov.
13. Committee on Capital Markets Regulation, *Interim Report of the Committee on Capital Markets Regulation*, November 30, 2006; available at www.capmktsreg.org/research.html.
14. AICPA, *Statements of Auditing Standards (SAS) Nos. 104–111. Risk Assessment standards, (New York, ASB*, March 2006); available at www.aicpa.org/Professional+Resources/Accounting+and+Auditing/Audit+and+Attest+Standards/Risk+Assessment.
15. AICPA, *SAS No. 82*: *Consideration of Fraud in a Financial Statement Audit* (New York: ASB, 1997); available at www.aicpa.org/download/members/div/auditstd/AU-00316.PDF.
16. AICPA, *SAS No. 84: Communication between Predecessor and Successor Auditors* (New York: Author, 1997); available at www.aicpa.org/download/members/div/auditstd/AU-00315.PDF.
17. Securities and Exchange Commission, ''The Private Securities Litigation Reform Act, 1995''; available at www.sec.gov.

Chapter 12

Governing Bodies

INTRODUCTION

In late January 2002, Tyco shares dropped sharply, one day after the company disclosed that a Tyco board member was involved with unapproved expenditures totaling $20 million. Subsequently, based on a tip, the New York County District Attorney issued a subpoena to Dennis Kozlowski, then Tyco chief executive officer (CEO).[1] On June 3, 2002, Kozlowski resigned unexpectedly as the *New York Times* reported that he was the subject of a sales tax evasion investigation by Manhattan District Attorney Robert Morgenthau's office. On June 4, Kozlowski was indicted.

The primary regulatory body for public companies is the Securities and Exchange Commission (SEC), which has civil lawsuit recourse only. Criminal indictments must be pursued by the Department of Justice. In Kozlowski's case, the local district attorney became involved. The regulatory and enforcement fabric related to financial malfeasance can be extensive.

Securities markets worldwide operate under the premise of fair transparent disclosure of information and protection of shareholder rights. Regulations are designed to achieve this premise, and stringent regulations are considered to provide higher investor protection at higher compliance costs. In Anglo-Saxon countries, securities regulations are intended to promote market efficiency and investor confidence where market participants have equal access to information, financial information is reliable, and there is a fair and level playing field. Regulations are designed to protect investors from receiving misleading financial information but are not intended to ensure that all investors make a desired return on investment. The safety, strength, and efficiency of capital markets determine the severity of the securities regulations, and differences in regulations across countries can be linked to differences in investor protections against unfair trading. Several governing bodies directly or indirectly influence corporate governance and the financial reporting process of publicly traded companies.[2] Regulatory challenges that transgress international boundaries are discussed later in the billion-dollar Satyam fraud. Exhibit 12.1 depicts governing bodies in corporate governance. This chapter presents the role of governing bodies in improving the quality, integrity, and reliability of financial reports.

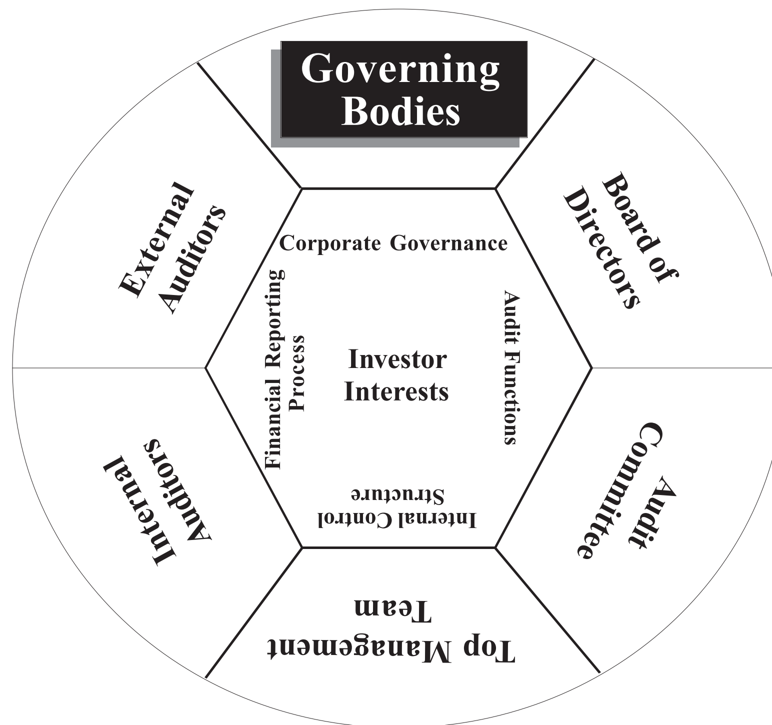


Exhibit 12.1 Corporate Governance and Its Functions

ROLE OF REGULATION IN CORPORATE GOVERNANCE

Regulatory reforms in the United States are aimed at improving the integrity, safety, and efficiency of the capital markets while maintaining their global competitiveness. In order to inspire investor confidence, regulations should be considered fair and in balance.[3] Fairness of regulations, while creating a level playing field for market participants, promoting investor protection and capital information, and ensuring that investors receive reliable information, does not guarantee success. Regulations should strike the right balance between not being so extensive as to discourage innovation, impose unnecessary costs on affected companies and their investors, or stifle competitiveness and job creation; and not being so lax to engage in a regulatory race to the bottom of eliminating necessary safeguards for investors. The Sarbanes-Oxley Act (SOX) of 2002 was enacted in July 2002 to restore investor confidence in public financial information in response to a wave of financial scandals at the turn of the twenty-first century.

Regulations, including SOX, are aimed at protecting the investors. The history of regulation in the United States appears to follow the pattern of lax regulation (early twentieth century) followed by corporate and accounting scandals (the stock market crash of 1929), followed by more regulation (Securities Acts of 1933, 1934),

relaxed or compromised regulation (end of the twentieth century), yet another wave of financial scandals (the late 1990s and early 2000s), and more regulation (SOX, SEC rules in implementing SOX provisions, listing standards of the early 2000s). The intent of regulation has been to restore public trust and investor confidence in corporate America, its financial reports, and capital markets pursuant to the occurrences of massive financial scandals. This endless cycle of financial scandals and government regulation is expected to continue; regulations often are compromised, leading to another wave of scandals. Regulation must be sustainable, cost-effective, efficient, and scalable to be effective in promoting investor confidence and market capital competitiveness, efficiency, and liquidity.

SARBANES-OXLEY ACT OF 2002

The three overriding goals of SOX are to restore investor confidence, enforce more accountability for public companies, and regulate corporate governance and the accounting profession.

Key provisions of SOX pertaining to corporate governance, financial reporting, and audit function are summarized in Exhibit 1.4 in Chapter 1. Some of the key provisions of SOX are that it:

1. Establishes the Public Company Accounting Oversight Board (PCAOB)
2. Prohibits auditors from performing nonaudit services contemporaneously with audit services
3. Requires publicly traded companies to have an audit committee composed of independent members of the board of directors
4. Requires the chief financial officer (CFO) and CEO to certify that financial reports do not contain any untrue statements and that they fairly present the company's financial condition and results of operations
5. Requires the CFO and CEO to be responsible for establishing, maintaining, and reporting on internal controls
6. Requires corporate executives to repay any bonus or compensation received if the company is required to prepare an accounting restatement due to material misstatements caused by fraud
7. Increases the prison sentences for wire and mail fraud and establishes a new category of crime for securities fraud to a 20-year sentence
8. Makes document shredding unlawful and a crime subject to prison
9. Ensures that corporate fraud is punishable regardless of when it is discovered
10. Requires the lead partner in charge of the audit and the audit partner responsible for reviewing the audit be replaced every five years
11. Directs the SEC to conduct a study of securities professionals who have been found to have aided and abetted a violation of federal securities laws

12. Authorizes the SEC to recognize any generally accepted accounting principles that are issued by a standard-setting body (e.g., the Financial Accounting Standards Board [FASB]) that is a private entity, governed by a board of trustees, and funded in a manner similar to the PCAOB

Some provisions of SOX- and SEC-related rules pertaining to strengthening the corporate board and external auditor independence, executive certifications of both financial statements and internal controls, and creation of the PCAOB to oversee the accounting profession have generated positive impacts for investors in terms of rebuilding their confidence in public financial information and the capital markets. SOX has created an environment under which public companies can effectively operate in achieving sustainable performance, being held accountable for their activities, and providing protections for their investors. Corporate governance reforms, including SOX, are needed to identify and manage conflicts of interest among market participants and bring more accountability and transparency into public financial reports.

Many of the provisions of SOX require the SEC and other regulators to establish additional regulations and rules (certification, disclosure controls and procedures, codes of ethics). Although the implications of some provisions are not immediately obvious (establishment of public company accounting oversight board, attorney reporting, audit committee), many provisions take effect currently (reporting requirements, senior executives' certifications, actions prohibiting fraudulently influencing an audit, and loans to directors and officers). These effects are expected to improve investors' confidence in capital markets, confidence that has significantly eroded in recent years. Therefore, investors will benefit from provisions of SOX and related SEC implementation rules. Implementation of provisions of SOX should have positive effects for essentially everyone directly or indirectly associated with financial reports or participating in the capital markets. Corporations can benefit from the implementation of provisions of SOX by improving corporate governance, quality and transparency of financial reports, and effectiveness of related audit functions, thus restoring public confidence in corporate America. Management can benefit by utilizing cheaper capital to improve profitability and, thus, higher bonuses, stock options, and other compensation plans. Investors, including shareholders and creditors, will benefit by being better able to assess the risk and return associated with their investment through more accurate and complete financial information. More reliable financial information disseminated to the capital markets can make the security markets more efficient and in turn can result in more effective allocation of the nation's resources and economic growth and prosperity.

SOX is reported to have a positive impact on business codes of conduct by moving them "from a rather loosely defined back-burner element of corporate governance to an element that is now explicit and far more prominent."[4] However, SOX is only one element in the complex corporate culture that determines the ethical conduct of participants (directors, officers, auditors, employees) in the current corporate business model. Changes in corporate culture in promoting competency

and integrity among all corporate governance participants are required. Effective implementation of provisions of SOX, in the areas of executive certifications of both financial statements and ICFR, creation of PCAOB in regulating the registered auditing firms and improving their audit quality and strengthening the audit committees' oversight effectiveness, is expected to reduce incidents of financial statement fraud.

Tyco: Extravagance to the Point of Abuse

Tyco manufactures a wide variety of products, from electronic components to health care products. The conglomerate operates in more than 100 countries and employs roughly 240,000 people. In the early 2000s, Tyco was a story of fraud and abuse. First, Frank Walsh, Tyco board member, received an unapproved $10 million finder's fee related to the March 2001 Tyco acquisition of CIT Group. Another $10 million went to a charity where Walsh was a director. The board of directors then launched an investigation. Although the company admitted no wrongdoing, it agreed to make pretax income adjustments in 2002 of $382.2 million.

The list of Tyco worst practices included:

- Poor documentation
- Inadequate policies and procedures to prevent misconduct by senior executives
- Inadequate procedures for proper corporate authorizations
- Inadequate approval procedures and documentation
- A lack of oversight by senior management at the corporate level
- A pattern of aggressive accounting

Tyco's board and management were also criticized for failing to set appropriate standards of ethics, integrity, and accounting and corporate governance.

Tyco provided the investing public with some of the most notorious examples of corporate excess. Kozlowski was noted as spending shareholder (Tyco) money on these items:

- $6,000 shower curtain
- $2,200 wastebasket
- $15,000 umbrella stand
- Approximately $1 million (of the $2 million total) for the cost of a birthday party for Kozlowski's wife, a Roman-themed extravaganza in Sardinia, the second-largest island in the Mediterranean Sea, which featured entertainers clad in togas and an appearance by singer Jimmy Buffett
- Kozlowski's New Hampshire home at three times the 2000 market value
- Money to charities in his name, using Tyco funds. (In one example, $1.3 million was "donated" to preserve the Squam Swamp in Nantucket, Massachusetts. As it turns out, the swamp was next to Kozlowski's own estate, and the donation prevented the swamp from being developed.)

Kozlowksi, CEO, and Mark Swartz, CFO, both received 8.33 to 25 years plus millions in fines. The men may fare poorly in prison because New York lacks a minimum-security facility and thus their time in prison may be harsh. Frank Walsh Jr., Tyco director, also pleaded guilty and acknowledged that he received a $20 million payment from Tyco for

helping to broker an acquisition. The external auditor agreed to pay $225 million to settle a class action lawsuit, and the company agreed to put $2.975 billion into a fund to settle most shareholder claims over the actions of Kozlowski and Swartz.

Sources: "Tyco Fraud," available at www.lawyershop.com/practice-areas/criminal-law/white-collar-crimes/securities-fraud/lawsuits/tyco. Jennifer Bayot and Andrew Ross Sorkin, "2 Tyco Officials Get Up to 25 Years for Fraud," *International Herald Tribune,* September 19, 2005. Stephen Taub, "Tyco on Tyco: Errors Made, but No Fraud," CFO.com, December 31, 2002.

SECURITIES AND EXCHANGE COMMISSION

Congress created the SEC to address, restore, and maintain investor confidence after the 1929 stock market crash. The SEC is an independent federal regulatory agency established through congressional legislation in 1934. The SEC has the authority to prescribe the form and content of financial statements of publicly traded companies. The Security Act of 1933 and the Securities Exchange Act of 1934 were enacted to protect investors' interests and to ensure that the capital markets are fair, honest, and efficient. These acts and related rules and regulations issued by the SEC require disclosures to be made in registration statements and prospectuses used in securities offerings as well as in annual, quarterly, and other public reports filed with the SEC.

SEC GOALS

The goals of the SEC include the following:

- Enforce compliance with federal securities laws by detecting problems in the securities markets, preventing and deterring violations of federal securities laws, alerting investors to possible wrongdoing, sanctioning wrongdoers, and returning funds to harmed investors.
- Promote healthy capital markets through an effective and flexible regulatory environment that facilitates innovation, competition, and capital formation, and improves investor confidence in the capital markets.
- Foster informed investment decision making by ensuring that investors receive complete, accurate, and transparent financial information and by implementing a variety of investor education initiatives.
- Maximize the use of SEC resources through improvements in its organizational and internal controls effectiveness and sound investments in human capital and new technologies.

The SEC has also been given statutory authority to issue accounting standards for companies under its jurisdiction. The SEC has delegated its standard-setting

authority to the private sector (e.g., FASB), while exercising the oversight function of the private sector's standard-setting processes and the right to override, supplement, and/or amend private sector standards. The SEC also plays an important role in the financial reporting process of registrants through its continuous monitoring of their accounting and reporting practices. The SEC has promoted high-quality financial reports free of material fraud through its continuous oversight functions, establishing security rules, and enforcement of its rules. Since its inception in 1934, the SEC has required publicly traded companies to comply with initial and continuing disclosure standards to prevent misleading or incomplete information and to foster informed decisions by investors.

Federal securities law prohibits financial statement fraud by publicly traded companies through mandated truthful financial disclosure. Rule 10(b)-5 of the Securities Exchange Act of 1934 prohibits disclosure of material untruths and omissions in open-market trades. The acts of 1933 and 1934 fundamentally constitute security market regulation in the United States. The provisions of these two acts protect investors from fraudulent or misleading information that may cause security price manipulation. In an efficient capital market, security prices reflect the market participants' (e.g., individual investors, analysts, institutional investors) expectations of future cash flows to shareholders. Financial statement fraud, by presenting misleading financial information, can adversely affect the market's expectations and, thus, security prices.

Since 1934, the SEC has been empowered by Congress to make rules and regulations governing registration statements and prospectuses and to issue accounting standards for registrants. Publicly traded companies under the SEC jurisdiction that issue misleading financial disclosures are in violation of Rule 10(b)-5 of the Securities Exchange Act of 1934. This type of violation constitutes a form of corporate illegal activity (fraudulent activity) subject to SEC legal enforcement procedures that can result in substantial economic losses to the corporation, its top executives, and its stakeholders (e.g., investors, creditors, employees, and customers). SEC has been criticized for exempting privately owned brokerage firms (e.g., Madoff; brokerage firms) from the SOX requirement of being audited by a registered public accounting firms subject to the routine inspection of the PCAOB. Madoff used an alleged $50 billion Ponzi scheme paying returns to an investor from money invested by another investor for more than 28 years.

The 1934 act is based on the premise that stock prices are susceptible to misleading financial information, manipulation, and control. The U.S. Congress has authorized the SEC to mandate periodic financial reports by publicly traded companies. These financial reports (annual or quarterly) were required in addition to registration statements, prospectuses, and proxies required by the 1933 and 1934 acts. These acts do three things:

1. Prohibit disclosure of false or misleading information and manipulation of fraudulent behavior intended to affect security prices

2. Impose explicit liabilities and penalties on fraudulent financial reporting activities
3. Disallow the use of nonpublic information by specialists and insiders

Thus, these acts affect company management and investor behavior by requiring that management publish reliable financial information and enabling investors to use that information in making capital investment decisions.

SEC's ROLE IN FINANCIAL REPORTING

The Securities Exchange Act of 1934 gave the SEC congressional authority to promulgate accounting policies and standards better known as generally accepted accounting principles (GAAP). The SEC has issued rulings called Accounting Series Releases (ASRs), Financial Reporting Series Releases (FRSRs), and Staff Accounting Bulletins (SABs) to specify acceptable accounting principles for companies under its jurisdiction. However, over the years and for the most part, the SEC has delegated its accounting standard-setting authority to the private-sector Financial Accounting Standards Board (FASB). The FASB has issued Statements of Financial Accounting Standards (SFASs) and related interpretations through a lengthy deliberation process in establishing GAAP for external financial reporting. During the past three decades, the SEC and FASB have worked closely together in establishing GAAP, with the SEC playing largely an oversight and supportive role.

The SEC's role in corporate financial reporting according to the Report of the SEC Advisory Committee on Corporate Disclosure[5] is to ''assure the public availability in an efficient and reasonable manner and on a timely basis of reliable, firm-oriented information material to informed investment and corporate suffrage decision-making.'' This overseeing responsibility of the SEC is presumed to assure ''the semi-strong capital market efficiency'' concept, which suggests that security prices reflect all available public information, including published financial statements. The SEC regulations of corporate financial disclosure are intended to prevent ''market failure.'' Brownlee and Young[6] argue that the notion of market failure has two fundamental components: the ''public good'' and ''asymmetry'' of information. The ''public good'' nature of corporate financial reports suggests that published corporate financial information is viewed to be public good primarily for three reasons:

1. The use of such information by one person does not reduce the quantity or quality of the information available to others.
2. Nonpurchasers cannot be excluded from consuming it.
3. Financial information passes both the joint consumption and nonexclusivity attributes of public goods.

Thus, proper SEC disclosure regulations are necessary to ensure that adequate financial information is produced and disseminated by corporations. In the absence of SEC-mandated financial disclosure, corporations may produce unreliable and insufficient financial information that may lead to suboptimal resource allocation

and resulting market failures. The public good concept of corporate financial information deals with the efficiency issue of the capital markets.

The second element of market failure related to the concept of "asymmetry" is the manner in which financial information is distributed among market participants. This asymmetry notion pertains to the equity issue of publicly available financial information. Asymmetry of financial information suggests that corporate insiders (e.g., management, board of directors) may know much more about their corporations than do outsiders (investors). This may provide opportunities for insiders to fraudulently take advantage of monopolistic information to influence stock prices. Thus, SEC regulations prohibit insider trading that may create inefficiency in the capital market. The SEC's new disclosure regulation (fair disclosure) is intended to create a level playing field for all market participants. Illegal insider trading has received considerable attention by the financial community and generated significant political interest. Thus, the Insiders Trading Sanctions Act of 1984 (Public Law No. 98-376) extended SEC enforcement powers regarding insider trading and imposed significant penalties on those found guilty of insider trading. The severity of the insider problems encouraged Congress to review the SEC's role in the supervision and issuance of accounting standards and the existing structure for establishing disclosure requirements for publicly traded companies.

Oil-for-Food

Oil-for-Food was a $64 billion program established by the United Nations in 1995 in the wake of the 1991 U.S.-Iraq War to allow Iraq to sell oil on the world market in exchange for food, medicine, and other humanitarian needs of its people and to repay war reparations. The program was designed for the benefit of ordinary Iraqi citizens who were unintended victims of the international economic sanctions aimed at Saddam Hussein's military. The program was discontinued in 2003, at the time of the second U.S.-Iraq War, when humanitarian functions were turned over to the Coalition Provisional Authority.

During its lifetime, allegations of fraud, abuse, and illegal kickbacks in the Oil-for-Food program were rampant. It is alleged that Saddam Hussein siphoned off at least $2 billion in illegal kickbacks. Subsequent investigations resulted in 14 persons being indicted.

Among the most notorious, South Korean businessman Tongsun Park was arrested in January 2006 for illegally accepting millions of dollars from Iraq. In July 2006, he was the first person convicted in the conspiracy. On February 22, 2007, he was sentenced to five years in prison, fined $15,000 and required to forfeit $1,200,000.

Most infamous is Benon Sevan, United Nations undersecretary and director of the Oil-for-Food program. Sevan was indicted for taking about $160,000 in bribes. His co-conspirator, Efraim "Fred" Nadler, a New York businessman and brother-in-law to UN Secretary General Boutros Boutros Ghali, was indicted on charges of channeling the illegal payments to Sevan.

Sources: Colum Lynch, "Former U.N. Oil-for-Food Chief Indicted," *Washington Post,* January 17, 2007. Colum Lynch, "Park Sentenced to 5 Years in U.N. Oil-for-Food Bribery Scandal," *Washington Post,* February 23, 2007.

SEC's REGULATION FAIR DISCLOSURE

The SEC has had great concern over selective disclosure of material information by financial information issuers for several years. Many publicly traded companies disclosed important nonpublic information, such as advance warnings of earnings results and restructuring changes, to securities analysts or selected institutional investors or both before they made full disclosure of the same information to the general public. The investors with access to the information before others either made a profit or avoided losses. On October 23, 2000, Regulation Fair Disclosure (FD) went into effect and became the law. The regulation banned the practice of holding conference calls with analysts by invitation only, also known as *selective disclosure.* The SEC proposed such a regulation to provide a more level playing field for those investors who do not have insider or early information on which to base their decisions. The reasons for the regulation are listed next:

- Certain analysts and individuals had access to information that was not available to the public.
- Assuming the securities markets are efficient, the markets will react to all public and nonpublic information.
- Some companies wanted to appear more profitable than they actually were by using the information to persuade analysts to provide inaccurate positive estimates.
- Technology, such as the Internet, allows information to be distributed much faster.

The SEC has adopted a series of rules, including Regulation FD, Rule 10(b) 5-1, and Rule 10(b) 5-2.[7] These rules are designed to address the issue of how a publicly traded company's financial records are required to be disclosed, and to whom and when. The need for this new set of regulations and rules came about because of the public demand to address what was seen as a loophole in the laws that prohibit insider trading. While it was (and still is) highly illegal for a private investor to make a stock purchase or sale based on information gathered from a personal contact within the management of a company, many people believed that the practice of allowing the same type of information to be disclosed to a certain group of analysts and to certain large fund managers also violated the intent of the law. Those who are not "in the loop" with these analysts often find that the value of their stock has been driven down because of the actions of these analysts. In other cases, the price has been driven too high; once the news disclosed to the analysts becomes public, the analysts are insulated from the risk and the average individual investor loses money.

Regulation FD provides several important benefits to investors and the securities markets as a whole. Now all investors receive more fair information disclosure, thereby increasing investor confidence in market integrity. Regulation FD, by

increasing market confidence, maintains and enhances extensive investor participation in the market, thus encouraging better market liquidity and efficiency while promoting more effective market capital rising. In addition, benefits from the regulation include unbiased analysis. All investors have the same access to material information as analysts. Analysts can express honest opinions without fear of being denied access to valuable corporate information, as their competitors. As a result of Regulation FD, other analysts do not have the competitive edge just because they say better things about issues.

FINANCIAL FRAUD DETECTION AND DISCLOSURE ACT OF 1992

This act amended the Securities and Exchange Commission Act of 1934 by adding a new Section 13A to improve fraud detection and disclosure of publicly traded companies. The legislation requires independent auditors to perform adequate audit procedures designed to provide reasonable assurance of detecting illegal acts that would have a direct and material effect on financial statements, identification of material related party transactions, and assessment of the company's ability to continue as a going concern. This legislation requires that, if external auditors detect a material illegal act that would directly affect financial statements, the auditor should inform the appropriate level of management and the audit committee. If management failed to take timely and appropriate remedial action and management's failure warrants either a departure from a standard auditor's report or a resignation from the audit engagement, then the auditor should report these conclusions directly to the board of directors. The company should inform the SEC within one business day of receipt of the auditor's report. Failure of the company to report to the SEC may force the auditor to resign from the audit engagement or to report the suspected illegalities to the SEC within one business day.

PRIVATE SECURITIES REFORM ACT OF 1995

The Private Securities Litigation Reform Act of 1995 (the Reform Act), amended the Securities Exchange Act of 1934 by adding Section 10A. Section 10A required that each audit under the Securities Exchange Act of 1934 include audit procedures regarding the detection of illegal acts and the identification of related parties. The Private Securities Litigation Reform Act of 1995 became law on December 22, 1995. The U.S. Congress overrode President Clinton's vote in passing this act. On November 3, 1998, President Clinton signed into law the Securities Litigation Uniform Standards Act of 1998 (Uniform Standards Act).

The three major provisions of the Private Securities Litigation Reform Act of 1995 are (1) the "fair share" proportionate liability rule, (2) the deployment of damage caps, and (3) the requirement for fraud detection and disclosure. King and

Schwartz discuss these three provisions of the act and present suggestions and strategies to address these provisions.[8] They conclude that auditors are required not only to detect illegal acts, including financial statement fraud, but also to determine an appropriate and timely remedial response for management.

The Health Care Paperwork Reduction and Fraud Prevention Act of 2001 was introduced on March 20, 2001, in the 107th Congress as H.R. 1128. The purpose of this act, among other things, is to (1) reduce the amount of paperwork, (2) prevent fraud and abuse through health care provider education, and (3) improve payment policies for healthcare services.

SEC AND FINANCIAL STATEMENT FRAUD

The Securities Exchange Act of 1934 requires financial disclosure to provide investors with adequate information to allow them to make rational economic decisions. The required disclosures were deemed necessary to prevent financial statement fraud. The SEC financial statement fraud activities can be classified in three different groups: (1) SEC fraud prevention activities, (2) SEC fraud detection activities, and (3) SEC fraud enforcement activities. Pincus, Holder, and Mock[9] conducted a survey of a large sample of management, including officers and directors, attorneys, internal auditors, and external auditors, to determine the effectiveness of the SEC policies and activities in preventing, detecting, and disciplining cases of financial statement fraud. They wanted answers to two questions: (1) How effective are current SEC policies/activities at preventing, detecting, and disciplining fraud? (2) What potential changes to current SEC policies/activities would be effective in improving fraud deterrence and detection? Most respondents (63 percent of internal auditors, 56 percent of external auditors, 51 percent of attorneys, and 40 percent of management) replied that financial statement fraud is a problem of moderate to critical proportions.

SEC FRAUD PREVENTION ACTIVITIES

The respondents generally believed the SEC's policies and activities related to financial statement fraud to be at least somewhat effective. Most stated that these five fraud prevention activities of the SEC are moderately to very effective: (1) establishment of securities registration requirements, (2) review of registration requirements, (3) establishment of financial reporting requirements, (4) ongoing reviews of quarterly/annual filing, and (5) publicity related to enforcement actions.

There were few significant disagreements among the four groups of respondents regarding the SEC fraud prevention activities. Management, internal auditors, and external auditors believed that the SEC's most effective fraud prevention policy and activity is publicity related to enforcement actions, whereas attorneys believed the establishment of financial reporting requirements to be the most effective prevention policy.

SEC FRAUD DETECTION ACTIVITIES

In their survey, Pincus et al. discussed six SEC fraud detection activities:[10]

1. Reviewing any publicly traded company receiving other than an unqualified opinion
2. Reviewing all 8-K reports on auditor changes or unusual events
3. Responding to and considering tips from informants
4. Monitoring registration statements
5. Addressing quarterly annual filings
6. Monitoring market activity

Although all four groups of respondents ranked the SEC's fraud detection activities as moderately effective, they all agreed that the SEC's most effective fraud detection activity is responding to tips from informants. Although, overall, agreement among the four groups was high, internal auditors rated the effectiveness of monitoring market activities lower than all the other groups; management ranked the effectiveness of monitoring quarterly and annual filings as very high; and attorneys ranked the effectiveness of reviews of other than unqualified opinions higher than all the other groups. The respondents expressed their concern that budget constraints limited the SEC's effectiveness in reviewing quarterly and annual filings.

SEC FRAUD ENFORCEMENT ACTIVITIES

Accounting and Auditing Enforcement Releases (AAERs) issued by the SEC are being used as a signal of potential misstatements of financial statements and a proxy for financial statement fraud by users of financial statements, including investors and creditors. The use of AAERs has three advantages:

1. AAERs are an objective means of identifying publicly traded companies with fraudulent financial reporting.
2. AAERs contain most financial statement fraud for companies with auditor litigation.
3. The nature of financial statement fraud is described in AAERs.

The only shortcoming of AAERs is that they limit the SEC enforcement actions, reflecting a specific SEC agenda for publicly traded companies. In their study, Pincus et al. examined seven SEC fraud enforcement activities:

1. Referrals of cases to the Justice Department or state prosecutor's office
2. Referrals of cases to state ethics boards or state boards of accounting

3. Litigation (e.g., actions brought under Rule 10(b)-5)
4. Administrative proceedings against accountants
5. Administrative proceedings against issuers of securities
6. Court injunctions against a company's officers, directors, or employees
7. Published reports of investigations

Most respondents from all four groups believed that all of these enforcement activities are moderately to very effective in preventing and detecting financial statement fraud, except for the referrals to state ethics or accounting boards; respondents believed these were, at best, slightly effective enforcement mechanisms.

SUGGESTED CHANGES TO THE SEC CURRENT SYSTEM

The respondents in the Pincus et al. study were asked to express their views on the effectiveness of 26 possible changes to the current SEC system. Four suggested changes received high rankings by all groups of respondents:

1. Stiffer penalties for those involved in cases of financial statement fraud
2. Requirements for audit committees for all publicly traded companies, and requiring that a majority of the audit committee be outside directors
3. The requirement that a majority of the board of directors be outside directors
4. The development by the SEC of red flag profiles to help spot cases for investigation

Several reports (e.g., Blue Ribbon Committee on Audit Committee, 1999, and O'Malley Panel on Audit Effectiveness)[11] have also addressed these changes. Most recently, in the wake of Madoff's Ponzi fraud scheme, the SEC has been criticized and its efficacy in preventing similar fraud is being questioned. Three changes are being suggested to improve SEC's efficacy:

1. Eliminating unnecessary branch offices by improving collaboration and coordination between state and federal intra- and interagency
2. Reestablishing enforcement priorities by focusing on organizations, institutions, and companies that are more exposed to and threatened by fraud
3. Employing those best equipped to detect fraud (forensic accountants) to detect, punish, and deter future corporate wrongdoers[12]

SEC ADVISORY COMMITTEE ON IMPROVEMENTS TO FINANCIAL REPORTING

The Advisory Committee on Improvements to Financial Reporting (CIFiR) submitted a progress report to the SEC. The CIFiR has been charged with examining the U.S. financial reporting system and making recommendations aimed at increasing

the usefulness of financial information to investors while reducing the complexity of the reporting system. The report contains 12 recommendations that are based on these five main themes:

1. Increasing emphasis on the investor perspective in the financial reporting system
2. Consolidating the process of setting and interpreting accounting standards
3. Promoting the design of more uniform and principles-based accounting standards
4. Creating a disciplined framework for the increased use of professional judgment
5. Taking steps to coordinate U.S. generally accepted accounting principles with International Financial Reporting Standards (IFRS)[13]

The Satyam Scandal: When Riding a Tiger, How Does One Get Off without Getting Eaten?

As briefly discussed in the prior chapter, Satyam Computer Services Ltd. is one of India's largest outsourcing companies, claiming to service one-third of Fortune 500 companies. On January 7, 2009, founder and CEO Ramalinga Raju wrote a letter to the Satyam board of directors, outlining a massive fraud. According to blogger Lawrence Cunningham, cash was report to exceed $1 billion but apparently stands at just $78 million.

Portions of Raju's letter to the Satyam board, as reported by MSN.com (January 7, 2009) are summarized next.

> It is with deep regret and tremendous burden that I am carrying on my conscience, that I would like to bring the following facts to your notice.
>
> The Satyam balance sheet as of September 30, 2008 has:
>
> (a) Inflated (non-existent) cash and bank balances;
> (b) An accrued interest which is non-existent;
> (c) An understated liability;
> (d) An overstated debtors' position (accounts receivable).
>
> In addition, September's quarterly revenues were materially overstated; profits were overstated by as much as 500%.

Finally, Raju admitted that the gap in the balance sheet arose from inflated profits over several years.

Raju closed his letter by saying: "I am now prepared to subject myself to the laws of the land and face the consequences thereof."

While the details are subject to investigation by qualified professionals, one of the interesting facets of the Satyam case is that Raju claims in his letter that he, his brother, the company's managing director, and their families did not benefit personally from the fraud.

Raju's last-ditch effort to salvage the failing Satyam was the acquisition of Maytas Properties and Maytas Infra. When the acquisition fell through in mid-December 2008, the end was near. Raju comments in his letter: "It was like riding a tiger, not knowing how to get off without being eaten."

Satyam is a major corporation, audited by an Indian affiliate of one of the Big Four. The company is required to adhere to International Financial Reporting Standards and comply with SEC registration guidelines for foreign filers.

In cases where sales are inflated, the offsetting balance sheet account is often accounts receivable. The fraudster's challenge is that receivables have to be collected from the customer, reversed, or written off. Recognizing that auditors will scrutinize receivables, Raju proceeded to the next natural step and treated the receivables as if they had been collected. For Raju, this created a new problem: inflated cash balances. Saytam appeared to be sitting on huge piles of cash. This is where many are confused. Cash is usually a balance that can be audited through confirmation of bank balances and examination of bank reconciliations. How did Raju dupe the auditors for so many years without having cash in the bank?

Blogger Lawrence Cunningham on January 8, 2009, noted that the Satyam fraud creates some challenges for regulators because Satyam listed its shares in the United States and was audited by a foreign affiliate of a large U.S. auditing firm, where the affiliate operates outside the scope of the U.S. Public Company Accounting Oversight Board. Also, the Securities and Exchange Commission has given strong consideration to the concept of mutual recognition: a policy allowing foreign firms, especially brokers but potentially companies, to access U.S. securities markets without U.S. regulatory oversight. Finally, a question of liability for U.S.-based public accounting firms has arisen. Do audit failures by foreign affiliates of U.S. auditing firms expose the U.S. firm to potentially crushing legal liability arising from awards outside the United States? Staggeringly large damage awards could place U.S. audit firms at risk of bankruptcy.

The Raju brothers who founded Satyam Computer Services have been interrogated and jailed, and Srinivas Vadlamani, who resigned as chief financial officer, was arrested as well, held on charges of criminal conspiracy, forging accounts, and cheating as part of the same case that has been registered against the Satyam founders.

Sources: MSN.com, January 7, 2009, "Founder of Indian Company Interrogated," *New York Times,* January 12, 2009.

ROLE OF THE FINANCIAL ACCOUNTING STANDARDS BOARD

The Financial Accounting Standards Board (FASB) has been the designated organization in the private sector for establishing standards of financial accounting and reporting since 1973. The SEC has delegated its accounting standard-setting authority to the FASB to establish authoritative Statements of Financial Accounting Standards to govern the preparation of financial reports. The mission of the FASB

is to establish and improve standards of financial accounting and reporting by providing guidance to be used by companies for the measurement, recognition, and reporting of financial transactions and economic events and final preparation of financial statements. To accomplish its mission, the FASB acts to:

1. Improve the usefulness of financial reporting by focusing on the primary characteristics of relevance, reliability, quality, comparability, and consistency
2. Keep standards current to reflect changes in methods of doing business or changes in the economic environment
3. Consider promptly any significant areas of deficiency in financial reporting that might be improved through the standard-setting process
4. Promote the international comparability of accounting standards concurrent with improving the quality of financial reporting
5. Improve the common understanding of the nature and purposes of information contained in financial reports[14]

The FASB develops broad accounting concepts and standards for financial reporting. It also provides guidance on implementation of standards. Concepts are useful to guide the board in establishing standards and in providing a frame of reference, or conceptual framework, for resolving accounting issues. The framework helps establish reasonable bounds for judgment in preparing financial information and increase understanding of, and confidence in, financial information on the part of users of financial reports. It also helps the public understand the nature and limitations of information supplied by financial reporting. Thus, the FASB's role in corporate governance is to provide the standards and concepts that publicly traded companies must observe in preparing and disseminating financial statements. The FASB's established accounting standards provide uniformity, consistency, and comparability in applying a set of commonly accepted accounting methods and procedures used to produce reliable, useful, and relevant financial information to the investing public for financial decision making.

The FASB deliberation process consists of a chain of events of technical agendas, research procedures, preliminary views, public hearings, exposure drafts, revised exposure drafts, and final statements of financial accounting standards. Accounting standards issued by the FASB are intended to enhance the relevance, usefulness, and reliability of the financial reporting process by providing guidelines for management in making accounting decisions and assisting users of published financial statements in assessing management's decisions.

MONITORING BY INVESTORS

Investors, particularly institutional investors, should be actively engaged in monitoring their companies' corporate governance and fundamental decisions. Investors should participate in important affairs and engage with companies where value can

be added to their investments. By virtue of their influence and power, institutional investors should intervene when ineffectiveness or breakdowns in corporate governance occur to assist in protecting sustainable shareholder value. Individual shareholders can change managerial directions and decisions through selling their shares when there is corporate underperformance. If the majority of shareholders follow suit, management will be forced to act. In the case of institutional investors where funds are indexed with limited ability to sell, institutional engagement in corporate governance is the only way to correct ineffectiveness in corporate governance.

The company's board normally communicates with shareholders to obtain their approvals on resolutions. Shareholders are also given the opportunity to address issues of their interest through specific shareholder proposals. Traditionally, shareholder proposals have been nonbinding; therefore, the board can choose to ignore them even if they receive a majority of favorable votes. In reality, for these proposals to be able to influence corporate governance, they should be binding. Recently, proxy voting advisors, such as Glass Lewis & Co. and Institutional Shareholder Services, have played some important role in influencing board agendas and the proxy process.

RATING AGENCIES

The efficiency, liquidity, and safety of the financial markets, both debt and capital markets, have been threatened by the downfall of Bear Stearns and billions in write-downs by high-profile financial institutions in 2008. These threats have significantly increased the uncertainty and volatility in the markets, which adversely affects investor confidence. Ineffectiveness and inefficiency of regulations have contributed to the recent credit crisis, and new regulatory structures are needed to restore trust in the markets. Furthermore, failures of regulators, standard setters, ratings agencies, financial institutions, and gatekeepers in overseeing financial reporting process add to the crisis.

In the aftermath of the financial meltdown in 2008, rating agencies were blamed for overstating ratings of troubled mortgage firms. These agencies have traditionally relied on others' due diligence and on what they have been told by securities issuers. The SEC may require disclosure of what the rating agencies are being told and the basis for their professional judgment in rating of asset-based securities. To mitigate rating agencies' potential conflicts of interest, the SEC would require rating agencies to release publicly all their ratings along with the basis for their ratings; such actions would bring transparency into the rating process for mortgage-backed securities and collateral debt obligations.

The SEC recognizes the significant impact the rating agencies have on investment decisions. The scope of credit agencies' clientele includes not only individual investors but also large public institutions, commercial and investment banks, investment companies, and many others. Even regulatory bodies have come to rely on credit rankings. Additionally, the debacles of Enron and WorldCom increased the concern that credit agencies were under only nominal supervision by regulators.

In order to address those concerns, the SEC added Section 15E of the Exchange Act.[15] According to the final rule, credit rating agencies will be required to register with the SEC, make public certain information to help persons assess their credibility, make and retain certain records, furnish the SEC with audited financial statements, implement policies to manage the handling of material nonpublic information and conflicts of interest, and abide the certain prohibitions against unfair, coercive, or abusive practices.

ANTIFRAUD APPLICATIONS FOR PRACTICE

As we have seen from the many examples of corporate abuse, persons who commit fraud are successful, intelligent persons in positions of significant trust. If the typical financial statement fraudster looks the American success story, how do we approach fraud detection and investigation? More important, what characteristics are we looking for in those persons who conduct investigations? A list of the 10 keys to successful fraud examination follows:[16]

1. *Critical thinking*. Critical thinking, sometimes referred to as lateral thinking or thinking outside the box, is a disciplined approach to problem solving. Critical thinking is used as a foundation to guide beliefs and actions. It is a process to generate information and lead to other ideas. It is also a habit based on intellectual commitment to use the thought processes to guide behavior. Given that one aspect of fraud is intentional concealment, critical thinking is a necessary first step in the investigative process.
2. *Professional skepticism*. In the professional setting, critical thinking is the equivalent of professional skepticism. Professional skepticism is a neutral but disciplined approach to detection and investigation. Professional skepticism has three main attributes:
   - **a.** A *recognition* that fraud may be present and that the perpetrator will be intentionally concealing the organization's true financial performance
   - **b.** An *attitude* that includes a questioning mind and a critical assessment of information, data, and analysis
   - **c.** A *commitment* to persuasive evidence for decision making, including tying down all loose ends
3. *Red flags*. Red flags are warning signals that demands attention. Red flags are synonymous with symptoms. The red flags of fraud may be divided into at least six categories:
   - **a.** Unexplained accounting anomalies
   - **b.** Exploited internal control weaknesses
   - **c.** Identified analytical anomalies where nonfinancial data do not correlate with financial data

   d. Observed extravagant lifestyles
   e. Observed unusual behaviors
   f. Anomalies communicated via tips and complaints

4. *The principle of evidence-based decision making*. *Black's Law Dictionary* defines *evidence* as anything perceivable by the five senses and any proof such as testimony of witnesses, records, documents, facts, data, or tangible objects legally presented at trial to prove a contention and induce a belief in the minds of a jury. Fraud examiners and forensic accountants build all cases on the evidence.

5. *Investigations centered on the elements of fraud.* Investigators have to deal with the problem of intent. Intent, like all aspects of the investigation, must be grounded in the evidence. In a fraud case, the challenge is that short of a confession by a co-conspirator or the perpetrator, evidence of intent tends to be circumstantial. Thus, the elements of fraud are critical to the investigative process. The elements of fraud include the act (e.g., channel stuffing), the concealment (hiding the act or masking it to look like something different), and the conversion (the benefit to the perpetrator), as you can see in Exhibit 12.2.

   Provided that the investigator has evidence that the alleged perpetrator committed the act, benefited from that act, and concealed his or her activities, it becomes more difficult for the accused to argue that he or she did not intend to cause harm or injury. Evidence of concealment, in particular, provides some of the best evidence that the act, fraud or otherwise, was intentional.

6. *The importance of nonfinancial data.* The power of using nonfinancial data to corroborate financial information cannot be overstated. *Nonfinancial data* refers to data from any source outside of the financial reporting system that can be used to generate an alternative view of business operations. Essentially, economists break the world into prices and quantities (p's and q's). Fraud professionals and forensic accountants use this same approach to evaluate expected business relationships. Once critical metrics have been dissected into prices and quantities, each can be evaluated for reasonableness to determine if

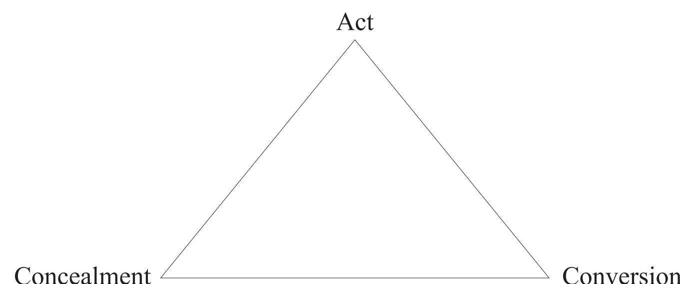


Exhibit 12.2 Elements of Fraud

the numbers make sense or whether further investigation is required. Nonfinancial data can then be correlated with numbers represented in the financial accounting system, financial statements and tax returns.

7. *Analysis of competing hypotheses*. In most fraud cases, it is unlikely that there will be direct evidence of fraud. There are rarely eyewitnesses, and, at least at the outset of the investigation, it is unlikely that the perpetrator will confess. Therefore, a successful fraud examination will take various sources of incomplete circumstantial evidence and assemble them into a solid, coherent structure that either proves or disproves the existence of the fraud. Like the scientist, the fraud examiner or forensic accountant postulates a theory based on observation and then tests it. When investigating complex frauds, the fraud theory approach is indispensable. Fraud theory begins with assumptions, based on the known facts, of what might have occurred. Then the theory is tested.

   Perhaps most important, professionals are always on the lookout for evidence that is inconsistent with their fraud theory. The analysis of competing hypotheses is a means of testing alternative hypotheses in an organized, summary fashion. One can never prove any hypothesis; in contrast, we can have two findings: (1) we have no evidence that directly refutes the most likely hypothesis (the fraud theory) and (2) we have evidence that seems to eliminate the alternative hypotheses.

8. *Importance of interviewing*. There is nothing more important to the successful resolution of fraud allegations than the ability to conduct penetrating and legally binding interviews of witnesses and suspects. Interviewing is the systematic questioning of a person who has knowledge of events, people, evidence, and other details surrounding a fraud or forensic accounting issue. In contrast, interrogation generally involves the questioning of suspects, targets, or uncooperative witnesses to obtain evidence, to obtain an admission of guilt or complicity in an act, or to give the interviewee an opportunity to volunteer facts and circumstances that may eliminate them as a suspect or target.

9. *Graphical tools*. Sometimes, the only way to figure something out is to draw a picture. More formally, fraud examiners use graphical tools to consider such questions as who knows who (linkages), who is connected with what business (linkages), how does the scheme work (flow diagram), who must be involved (links and flows), and what are the important events (timelines). Graphical analysis provides three beneficial outcomes: (1) the ability to identify critical questions that the investigation still needs to answer, (2) the ability to demonstrate the answers to critical investigative questions, and (3) the ability to draw conclusions.

10. *Importance of the story line: who, what, where, when, how, and why*. To be successful, the investigator must be able to explain to prosecutors, attorneys, juries, judges, and other actors in the investigative process the outcomes of the investigation: who, what, when, where, how, and, optimally, why.

The last thought:

Government is never so noble as when it is addressing wrongs.

—William Weld, the Republican Governor of Massachusetts from 1991 to 1997.

NOTES

1. www.lawyershop.com/practice-areas/criminal-law/white-collar-crimes/securities-fraud/lawsuits/tyco.
2. Securities and Exchange Commission, *Selective Disclosure and Insider Trading* (2000); available at www.sec.gov/rules/final/33-7881.htm#P14_1382.
3. H. M. Paulson, ‘‘Remarks by Treasury Secretary on the Competitiveness of U.S. Capital Markets, Economics Club of New York,’’ November 20, 2006; available at www.treas.gov/press/releases/hp174.htm.
4. D. Wallace, ‘‘What Has SOX Done for Us Lately?’’ *Sarbanes-Oxley Compliance Journal* (October 8, 2007); available at www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=2002.
5. Security and Exchange Committee (SEC), 1977. ‘‘Report of the SEC Advisory Committee on Corporate Disclosure, 1977’’; available at www.sec.gov.
6. E. R. Brownlee and S. D. Young, ‘‘The SEC and Mandated Disclosure: At the Crossroads,’’ *Accounting Horizons* (September 1987): 17–24.
7. Securities and Exchange Commission, ‘‘Selective Disclosure and Insider Trading,’’ August 8, 2000; available at www.sec.gov/rules/final/33-7881.htm#P14_1382.
8. R. King and R. Schwartz, ‘‘The Private Securities Litigation Reform Act of 1995: A Discussion of Three Provisions,’’ *Accounting Horizons,* November 1, 1997, 92–106.
9. R. V. Pincus, W. W. Holder, and J. Mock, ‘‘The SEC and Fraudulent Financial Reporting,’’ *Research in Accounting Regulation* 2 (1988): 167–185. All citations to the Pincus study refer to this work.
10. R.V. Pincus, W.W. Holder, and J. Mock 1988, ‘‘The SEC and Fraudulent Financial Reporting.’’ *Research in Accounting Regulations* 2: 167-185
11. Joseph Wells, Mary-Jo Kranacher, and Richard Riley, *Fraud and Financial Forensics* (Hoboken, NJ: John Wiley & Sons, forthcoming). Public Oversight Board, *Panel on Audit Effectiveness Report and Recommendations* (Stamford, CT: Author, August 2000).
12. M. Morgenstern, ‘‘Legislation Won’t Prevent the Next Madoff: SEC Needs Talent, Technology and Collaboration (Not New Laws),’’ The Huffington Post.com, January 13, 2009; available at www.huffingtonpost.com/marc-morgenstern/legislation-wont-prevent_b_15686.html.
13. Advisory Committee on Improvements to Financial Reporting to SEC, *Final Report of the Advisory Committee on Improvements to Financial Reporting to the United States Securities and Exchange Commission* (August 1,2008), Washington DC, available at www.sec.gov/about/offices/oca/acifr/acifr-finalreport.pdf.
14. FASB, ‘‘The Mission of the Financial Accounting Standards Board’’; available at 72.3.243.42/facts/index.shtml.

15. SEC, Final Rule, 17 CFR parts 240 and 249b, ‘‘Oversight of Credit Rating Agencies Registered as Nationally Recognized Statistical Rating Organizations,’’ Vol. 18, Number 116 (June 18, 2007): 6378–6431; available at www.sec.gov/rules/final/2007/34-55857fr.pdf.
16. Wells, Joseph, Mary-Jo Kranacher, and Richard Riley, *Fraud and Financial Forensics* (Hoboken, NJ: John Wiley & Sons, Forthcoming).

Part Four

Digital (Computer) Approaches to Fraud and Forensic Accounting

Chapter 13

Fraud in a Digital Environment

INTRODUCTION

A-Z is well spoken, business-savvy, and discreet. He is one of Russia's bright young tech stars, a crack programmer, successful entrepreneur, and creator of sophisticated software tools that help his customers make millions.[1] A-Z is also a cybercriminal, and his customer base is mostly unsavory characters. Cybercrime is fast expanding, global, and more lucrative than ever. Some experts in the tech security community estimate that cybercrime losses top $100 billion annually, outpacing global drug trafficking.[2]

The story of A-Z is part of a broader phenomenon referred to as ''NetWar,'' a concept first outlined by John Arquilla and David Ronfeldt of the RAND National Defense Research Institute. NetWar reflects many threats we face: asymmetric, networked, and adapted to the information age.[3] The distinguishing element of NetWar is network, not technology. However, the electronic information revolution is making networked organizations more effective because the conflict depends on and revolves around information and communications. The bad actors can be dispersed into small groups who agree to work together for a common cause or purpose; the participants may or may not know each other and may have ''met'' only through cyberspace. This facilitates easy joining of skilled resources from around the globe without geographical restrictions or requirements. While NetWar is not solely about technology, it does take advantage of technology: telephone, fax, e-mail, electronic billboards, chat rooms, instant messaging, blogs, and conferencing systems.[4]

The backbone of the U.S. economy is digital: communication devices, the Internet, and advanced computing technology. To take full advantage of this emerging digital economy, businesses are employing business-to-business (B2B) and business-to-consumer (B2C) e-commerce by developing Web sites with internal resources that integrate long- and short-term organization goals and the scope and scale of e-commerce operations focusing on security, privacy, and other risk management issues. The primary purposes of this chapter are to discuss the emerging digital economy, examine electronic financial reporting, discuss risks associated with electronic business and financial reports, and examine fraudulent financial activities involved in the electronic financial reporting process.

DIGITAL ECONOMY

During the past decade, there has been unprecedented growth in e-commerce. The Internet has revolutionized the way businesses do business, from the acquisition and serving of customers to receiving payment electronically. Organizations are constantly discovering new ways to deliver products and services electronically. E-commerce is being viewed as an important factor for economic growth in the twenty-first century. The emerging digital economy has received significant attention by regulators and policy makers. Two facets of the digital economy are electronic commerce (which uses the Internet or some other nonproprietary, Web-based system) and the information technology (IT) advances that enable e-commerce.

THE INTERNET

The advent of these Web browsers increased the use of the Internet for financial transactions at an exponential rate worldwide. The use of e-mail as a means of electronic communication can affect business decisions. Thus, the accuracy and integrity of information communicated through e-mail can be a major contributing factor in determining the reliability of financial information. E-mail messages, particularly those without digital signatures, can contribute to the occurrence of fraudulent financial activities and misappropriation of assets. For example, the Melissa and Love Bug viruses have caused billions of dollars in damages worldwide. The Emulex e-mail hoax that contained misinformation about a company's financial prospects caused a substantiated drop in the company's stock prices.[5] The perpetrators who send viruses and financial misinformation can significantly damage the quality, integrity, and reliability of financial reports. The Emulex hoax was an electronic fraud perpetrated against the company Emulex; a significant drop in the company's stock price and the disappearance of millions in market capitalization occurred within a few hours after a fraudulent and misleading e-mail message was sent to Internet Wire, a news service. The fraudulent news release stated that Emulex's chief executive officer was resigning because of the possible enforcement action by the Securities and Exchange Commission (SEC) regarding the company's accounting practices. Emulex's stock fell by approximately 61 percent, and market capitalization of more than $2 billion was lost. The fraudulent news release was sent by a former employee of Internet Wire for personal financial gain. The perpetrator was eventually caught and sanctioned.

INFORMATION TECHNOLOGY

Information technology has changed and will continue to change every facet of our lives, from the way we live, to how we work, to how companies do business, to how communication and information are being transformed. Technological advances, including the Internet and the use of e-commerce, have drastically changed the

way business is done and how decisions are made by management and other users of financial reports. Accounting and financial reporting that provides relevant, useful, and reliable information to support decision making should also change to better serve decision makers. During the past decade, the financial reporting process has evolved from a manual process of business transactions and hard copy of financial reports to a computerized process and electronic version of financial reports to most recently advanced electronic financial reporting and online, real-time financial reports. Indeed, on December 18, 2008, the SEC voted to require public companies and mutual funds to use interactive data for their financial reporting. The SEC unveiled its new financial reporting system called IDEA (Interactive Data Electronic Applications) to accept interactive data filings and provide investors with faster and easier access to key financial information. The evolution of the financial reporting process indicates a shift away from static financial statements presented once a year to dynamic electronic financial reporting developed online and in real time. Electronic financial reports are intended to be more dynamic, relevant, current, complete, and comprehensible.

eBay, a Technology of Choice for Bad Guys

Stealing merchandise has been a tried-and-true "professional endeavor" of criminals. However, selling the stolen goods has been a challenge, and the rewards were not always so good. Prior to the advent of the Internet, criminals hocking their stolen wares on the streets and in back alleys could expect to receive only $0.10 on the retail dollar. Not so with the advent of eBay. According to the *Washington Post*, bad guys offering their stolen goods on eBay can expect to receive as much as 76 percent of retail. Thus, thieves' gross margins have increased from 10 to 76 percent, a 660 percent increase as a result of the effective use of technology.

Source: Ariana Eunjung Cha, "Thieves Find Exactly What They're Looking for on EBay," *Washington Post,* January 6, 2005.

ELECTRONIC COMMERCE

E-commerce has already revolutionized the way business is conducted and the way organizations advertise, market, and sell their products and services. E-commerce is broadly defined as conducting business communications and transactions over computer-mediated networks. Exhibit 13.1 describes the types of e-commerce and their related strategies.

Next is a list of e-commerce strategies:

- *Business-to-business* (B2B) refers to online exchange of products and services involving transactions between businesses and suppliers (e.g., CISCO).

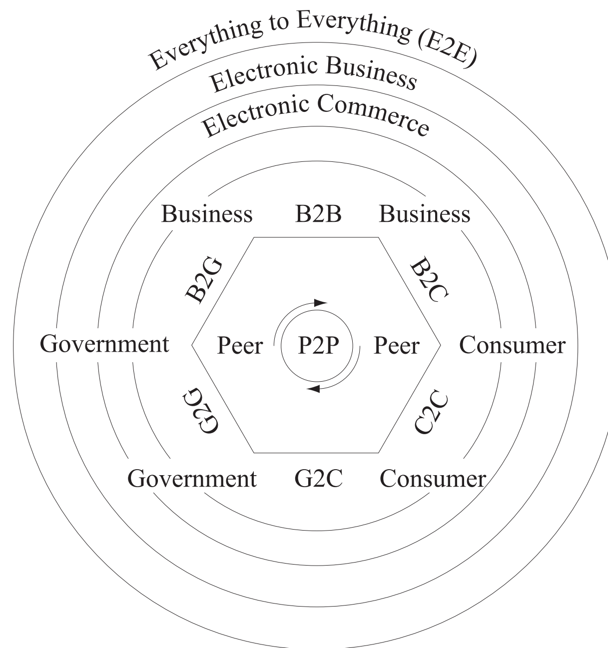


Exhibit 13.1 Electronic Commerce Strategies

- *Business-to-consumer* (B2C) is an online strategy of business dealing directly with consumers (e.g., Amazon.com).
- *Consumer-to-consumer* (C2C) is an online strategy of consumers dealing directly with consumers (e.g., eBay).
- *Business-to-government* (B2G) deals with electronic transactions between businesses and governmental agencies local, state, and federal.
- *Government-to-government* (G2G) e-commerce strategy includes all online programs and activities between government agencies (e.g., electronic transfer of funds and direct deposit).
- *Government-to-consumer* (G2C) refers to online transactions between governmental agencies and consumers (e.g., electronic transfers of state subsidy checks).
- *Peer-to-peer* (P2P) relates to sharing of computer capabilities between application platforms.

E-commerce strategies and related transactions are presented in Exhibit 13.2. E-commerce has provided businesses with many opportunities to save costs and continuously improve their performance. Customers can log on to a company's Web site to shop for their products and services. Companies are able to accept orders online and payment electronically. Thus, e-commerce facilitates expediting orders, invoices, acknowledgments, and payments. The emerging e-commerce arena is so

Exhibit 13.2 E-Commerce Strategies and Transactions

Type	Description
Business-to-business (B2B)	Businesses establish B2B capabilities through vendor-provided services and/or in-house resources.
Business-to-consumer (B2C)	B2C offers companies opportunities to (1) improve communication and information management within the organization and with customers; (2) lend innovation and growth; and (3) increase the bottom line.
Consumer-to-consumer (C2C)	C2C refers to an online strategy of consumers dealing directly with consumers such as online auctions (eBay).
Business-to-government (B2G)	B2G creates capabilities for companies to conduct online business with a wide variety of governmental agencies through an online auction to ensure competition (e.g., online government contracts with businesses replacing traditional sealed-bid auctions versus the online auctions).
Government-to-consumer (G2C)	G2C provides opportunities for governmental agencies to disseminate information online, effectively, and efficiently (e.g., registering voters or cars, electronic transferring of state subsidy checks, and purchasing government-issued licenses online).
Government-to-government (G2G)	G2G fosters online intergovernmental and activities between government agencies (e.g., digitized requests between agencies or employees for travel reimbursement).

significant that the White House has appointed an e-commerce senior advisor to focus on the developments, opportunities, challenges, and significance of e-commerce in our society today.[6] Businesses of all sizes and in all industries can benefit from the proper use of e-commerce. Small businesses can benefit from e-commerce to compete with larger companies for the same market or to reach out to the global marketplace. Large businesses need e-commerce to maintain their market share in the global marketplace, promote continuous growth, and reach new markets.

Welcome to the New World!

A-Z's (discussed in the introduction) computer program called ZeuS helps cybergangs steal people's identity data and pull off Web scams on a vast scale. In fall 2007, ZeuS was used to hijack $6 million. In prior eras, hackers let loose Internet viruses and hacked corporate computers for bragging rights. Here is the ''short-story'' version of how A-Z and his compatriots stole $6 million.

1. In summer 2007, a German gang skilled at pilfering online bank accounts forged a ''partnership'' with Russian hacker A-Z, who created ZeuS, a versatile software tool for infecting PCs that is housed on a network server in Turkey.

(*continued*)

The partnership sent out waves of e-mail spam carrying purported links to greeting cards, news stories, and celebrity videos. Clicking on the hoaxed link installed generic ZeuS on your PC. Generic ZeuS has two tasks: collect data typed on banking and other Web pages; and turn the PC into a "bot" that can be operated by other PCs remotely without the knowledge of the user.

2. The summer and fall was spent "harvesting" personal data from PC users with commercial accounts at banks that allow online cash transfers.
3. Targeted "fake" e-mail was sent to bank patrons asking them to "click here" to reset their security codes. The thousands who fell for the ruse had a custom version of ZeuS installed on their PC.
4. Custom ZeuS tracked the PC user's keystroke activity and alerted the cybergang each time PC users logged into their bank account. While users were logged into their banks, one of the cybergang's bots completed a cash transfer ranging from $5,000 to $10,000 in a few seconds without the users' knowledge.

A-Z is believed to be male, in his early 20s, living in Moscow. Within two weeks, the cybergang extracted $6 million from thousands of accounts at 20 of the largest banks in the United States, United Kingdom, Italy, and Spain. Authorities finally discovered the computer server holding key instructions for transferring funds in Turkey and shut it down. This is the essence of NetWar: cybercriminals from Russia, Germany and Turkey loosely combining for a short period to victimize banks and persons in the United States, England, Italy, and Spain.

NetWar allows bad actors to operate from jurisdictions where they remain largely free from concerns about punishment while taking advantage of victims anywhere in the world, targeting persons in more developed jurisdictions with substantial economic assets. NetWar participants can spend as much time as necessary to watch and wait and then swarm into action when opportunities arises. The "organization" can disappear just as quickly as it came to life.

Not only do nations but organizations need to be cognizant of and prepared to deal with these nontraditional forms of attack. Successful attacks affect the victim organization's reputation as well as place its customers, vendors, suppliers, employees, and other stakeholders at risk. Such attacks can cripple an organization. With regard to financial statement fraud more specifically, cybercriminals can look to destroy transactional databases and harvest valuable and sensitive information and communications that may have the effect of making financial statements materially misstated.

Source: SecureWorks and Alejandro Gonzalez, "Anatomy of a Cyber Bank Heist," *USA Today,* August 5, 2008.

CHANGES IN BUSINESS ENVIRONMENT

To understand why current business reports may not be value relevant and may not be as useful for financial decision making, it is necessary to analyze and understand the changes that have been taking place in business and how these changes have impacted information needs of users of business reports. The three fundamental changes in the business environment are:

1. Technological advances
2. Globalization of economy and business
3. Convergence in the financial and capital market

The next sections examine these three changes in the business environment and their impacts on the financial reporting process.

INFORMATION TECHNOLOGY

Today's business increasingly is driven by IT. Technology has not only rewritten the rules of business but also has made information preparation and dissemination inexpensive. Technological advances, including the Internet, include low-cost, high-speed digital data transmission that uses hardware that produces information quickly and easily and uses software that reduces and, in many cases, eliminates much of the time, space, and other constraints to information. The progress in IT, while reducing both transaction costs and asymmetric information problems, has increased economies of scale and scope in all business sectors. Applying the lessons of NetWar to business, technology—including e-commerce—provides both businesses and customers with a greater degree of information efficiency.

GLOBALIZATION OF ECONOMY AND BUSINESS

Globalization is the most extensive and profound challenge facing the business community in the United States and abroad. The challenges of globalization compel the business community to better understand why and how major international events and developments affect business practice and conduct. As the business environment becomes more globalized, businesses are forced to face and respond to increasing international challenges and opportunities. Online, real-time, and instantaneous information coupled with efficient and effective methods of transportation have enabled the world to become one giant marketplace. E-commerce enables businesses and consumers to buy products and services through the Internet in the global market as readily as they can from a local business.

CONVERGENCE IN THE FINANCIAL AND CAPITAL MARKET

Convergence within the industry (e.g., the financial services industry among banks, insurance companies, mutual funds, and brokerages) has significantly affected the relationship between the company and its investors. Convergence across industries has also changed financial reporting and relationships with financial markets and major market players.

The logic of a universal financial service (e.g., one-stop shopping for all financial services and products) offering a variety of financial products and services is compelling. Universal banking (banc assurance) has been practiced in Germany,

Canada, and other countries, but, until recently, it has not been permitted in the United States. The Gramm-Leach-Bliley (GLB) Financial Modernization Act of 1999, which officially went into effect in March 2000, permits banks, securities firms, insurance companies, mutual funds, and brokerage firms to freely enter each other's business or consolidate.[7] The act allows creation of financial holding companies that may conduct a broad range of financial services, including insurance, securities underwriting, commercial banking, asset management, merchant banking, and real estate development and investment. The recent wave of consolidations in the financial services industry has resulted in fewer but larger financial services organizations. Traditionally, the financial services and products of banks, insurance companies, mutual funds, and brokerage firms were distinguishable and their roles were separated. Today, the differences among functions of these financial services providers are becoming less noticeable.

The 12 provisions of the GLB act are summarized next:[8]

1. Permits commercial banks to affiliate with investment banks
2. Allows companies that own commercial banks to offer all types of financial services
3. Permits subsidiaries of banks to offer a broad range of financial services that are not allowed for banks themselves
4. Creates financial holding companies (FHCs) that may conduct a broad range of financial activities including commercial banking, insurance and securities underwriting, and merchant banking, as well as real estate development and investment
5. Establishes restrictions on the locations of the new or expanded nonbank financial activities within the banking organizations
6. Permits financial holding companies to conduct activities that are complementary to banking
7. Grandfathers for 10 years the nonfinancial activities of firms predominantly engaged in financial business, with the possibility of a five-year extension
8. Establishes the Federal Reserve Board as the primary regulator of financial holding companies
9. Provides for functional regulation of financial activities by state and other federal agencies
10. Gives the Treasury Department and the Federal Reserve the right to veto each other's decisions on new financial powers
11. Requires financial institutions to establish privacy policies to prevent disseminating information about customer accounts to third parties. These policies should be disclosed at the start of a customer relationship and once a year thereafter
12. Affects the implementation of the Community Reinvestment Act of 1977 (CRA), including the requirement that a bank holding company cannot become

a financial holding company unless all the company's insured depository institutions have a CRA rating of at least satisfactory

The passage of the GLB act has raised some concerns that its implementation may concentrate economic power in the financial services industry, which would make it more difficult for government to oversee the industry's activities and strategies in managing risk, and cause more exposure for improper safeguarding of customer information and consumer financial privacy. To address those concerns, the GLB act requires that the Federal Reserve have ''umbrella'' supervisory authority over financial holding companies and establishes four privacy provisions for sharing of customer information with others and protecting the privacy of customers' information. Specifically, the GLB act requires financial services organizations to:

1. Establish and annually disclose a privacy policy
2. Provide customers the right to opt out of having their information shared with nonaffiliated third parties
3. Not share customer account numbers with nonaffiliated third parties
4. Abide by regulatory standards to protect the security and integrity of customer information

Internal auditors can take an important proactive role in safeguarding customer information and ensuring consumer financial privacy in compliance with the requirements of the GLB Act.

E-Discovery

On December 1, 2006, a series of amendments and revisions to the Federal Rules of Civil Procedure (FRCP) went into effect. These changes recognize the unique nature of electronically stored information and lay out guidelines and requirements for storing and disclosing electronic information during litigation. In short, *electronic discovery* (e-discovery) refers to any process in which electronic data are sought, located, secured, and searched with the intent of using the data as evidence in a criminal or civil legal case. If companies do not properly track the information stored in various files, e-mail, and documents and if that information is required as evidence in a court case, the organization could face major fines and consulting fees to compensate professionals for locating the required electronic data.

The revised rules require systematic archiving and preservation of electronic information so that it can be produced in a format that is easily readable if requested by the opposing party during ''discovery,'' the process whereby opposing counsel shares information that may be deemed suitable for presentation at trial. Companies need to put policies and procedures in place that outline what data must be retained and set up mechanisms for instituting these policies. Data of all types can serve as evidence, including text, images, calendar files, databases, spreadsheets, audio files, animation, Web sites, and computer programs.

(*continued*)

Electronic mail communications (e-mail) can be an especially valuable source of evidence because people often are less careful and more candid in these exchanges than in hard-copy correspondence.

The nature of digital data makes it extremely well suited to investigation. Digital data can be searched electronically with ease, whereas paper documents must be scrutinized manually. Furthermore, digital data are difficult, if not impossible, to completely destroy. This is because data often appear on multiple hard drives and because deleted files can often be undeleted.

Sources: ‘‘Amendments Approved by the Supreme Court - Submitted to Congress (April 2006),’’ available at www.uscourts.gov/rules/congress0406.html. ‘‘Coping with New E-Discovery Requirements,’’ LexisNexis for Associates. Elizabeth Montalbano, ‘‘New Rules Open the Way to eDiscovery,’’ *InfoWorld*, October 25, 2006.

ELECTRONIC FINANCIAL REPORTING

The currently prepared and disseminated Web-based financial reports are exact electronic reproductions of the printed annual reports. Practically, they are electronic duplications of the traditional printed financial reports with no value added except they are readily available. Animated graphics, videos, and sound Web-based financial reports, while improving the look and feel of information, add nothing to the usefulness of the information. Use of the Internet in the electronic financial reporting process should go beyond speed and accessibility and the next level of providing navigation through the information and making it readable by several application resources for a wide variety of purposes. The extensible business reporting language (XBRL) format is designed to accomplish this advanced level of using the Internet in the electronic financial reporting process.

Web-based reports offer many advantages to investors, creditors, and other users of financial information. The Web is relatively inexpensive and facilitates a quick way to communicate with many users electronically; however, no standard currently exists for reporting information on the Internet, and it is often difficult to find accounting data for particular companies on the Web. The evolution of the financial reporting process in the United States indicates a steady but slow move away from the paper-based historical financial reports to online reporting of historical financial reports on Web sites, to online reporting of financial reports in Hypertext Markup Language (HTML), which allows for linking one section of the report to other relevant sections and documents, and to more advanced, reactive, online reporting by using extensible markup language (XML) and its financial offspring, XBRL, to make financial information more interactive and consistent.

Publication of financial information in the XBRL format can save significant amounts of time and cost in preparing and disseminating financial information, as well as in searching and exploring information into other XML-aware applications.

The first XBRL taxonomy is intended for commercial and industrial companies reporting according to U.S. generally accepted accounting principles (GAAP). XBRL taxonomy is a classification and directory of financial statement items and definitions that meet the requirements of the overall XBRL specification. This directory describes each data element by a specific type of business entity in the specified industry. The XBRL taxonomies have already been developed for U.S. mutual funds, U.S. federal entities, and commercial and industrial companies that use standards set by the International Accounting Standards Committee (IASC). The use of IASC taxonomy enables a global implication, adoption, and implementation of XBRL.

Further development of XBRL taxonomies for different industrial sectors (i.e., commercial, financial institutions, governmental agencies, and nonprofit organizations) will promote the use of standardized and electronic financial statement fraud detection approaches and applications. Electronic financial reports published on the Web and the Internet provide an opportunity to identify visible factors (red flags) that signal the likelihood of the occurrence of financial statement fraud.

BENEFITS OF XBRL

XBRL offers many benefits to a variety of users, including investors, analysts, companies, industries, software, vendors, and publishers of financial statements. Much of the demand for XBRL comes from investors, creditors, and other users of financial reports. Under the XBRL format, they are able to extract, analyze, and process electronic financial statements on a more efficient and timely basis. Because XBRL enables a variety of formats, investors, creditors, and other users of financial reports can receive the information they prefer in a specific style of analysis. Furthermore, by making financial information available on corporate Web sites via XBRL, investors who have a reasonable understanding of financial reporting can obtain the desired financial information constantly and on a real-time basis.

XBRL lowers the cost of preparing and disseminating financial statements. Currently, publicly traded companies typically prepare three sets of financial statements: one for external release, one to be filed with the SEC, and one to post on the company Web site. Under the XBRL format, financial statements will need to be prepared only one time to be printed, posted on the Web, or filed with the SEC. This one-time processing and preparation of financial reports in serving a broad range of purposes should reduce the opportunity for manipulation of financial information and, accordingly, reduce the likelihood of financial statement fraud.

XBR is an open language that offers independent software vendors an incentive to incorporate XBRL into their applications to enhance the usability of this software. Thus, virtually any software product that manages financial information could use XBRL to import and export additional formats. Although XBRL enables users of financial statements to exchange financial information electronically, financial statement publishers and other data aggregators will experience reduced operating costs associated with more efficient data collection and a reduction of errors.

Preparers and users of financial reports can take advantage of these benefits offered by using the XBRL format for the financial reporting process:

- It can be built into financial and accounting software free of charge, which allows the automatic exchange and reliable extraction of business information across all software formats and technological platforms, including the Internet.
- It makes the preparation, dissemination, and analysis of financial reports more efficient and effective.
- It provides more relevant and reliable information by allowing for technology independence, less human involvement, and more reliable and efficient extraction of financial information.
- It makes financial information more readily available and less expensive by providing faster, more accurate electronic searches for information.
- It creates opportunities for online, real-time accounting systems with a standards-based method of preparing, disseminating, extracting, and analyzing financial information.
- It makes it easier for those with less technological competence to take advantage of powerful tools.
- It enables reporting from multiple locations and departments, which ultimately benefits all users of the financial information supply chain.
- It permits better communication within the financial reporting chain (e.g., shareholders, suppliers, auditors, lenders, employees, governmental agencies).
- It enables plug-and-play systems by creating opportunities to have authentic ‘‘roll your own,’’ best-of-breed interoperable systems without having to disclose any additional information beyond what is required under the current accounting standards.
- It empowers internal audit functions with new tool sets for analytical and related risk management issues.
- It creates smooth information flow by:
  - Reducing the need to enter financial information more than one time
  - Reducing the risk of data entry error
  - Eliminating the need to manually key information for various formats
- It applies to all managerial and financial philosophies and concepts, including just-in-time (JIT) inventory planning and controlling, activity-based costing (ABC), balanced scorecard, and value reporting.

CHALLENGES OF XBRL

The challenges of XBRL for publicly traded companies are as follows:

- Security
- Future of XBRL
- Scope
- Continuous assurance
- Fair disclosure
- Privacy
- Trust
- Implementation of the XBRL-based reporting system

Security

Electronic financial reporting has created unprecedented security issues that should be addressed to secure the integrity and quality of XBRL-generated information and trust, as well as confidence, in electronic transactions. Organizations should ensure that XBRL-prepared and disseminated information is properly safeguarded. The risk of fraud in electronic financial reports is real and can be substantial for businesses. To reduce the risk of fraudulent electronic financial reports, several significant technologies have been developed to validate, authenticate, and secure electronic transactions.

The considerable threat of security breaches encourages software developers such as Microsoft to develop Designing Secure Web-based Applications for operating platforms such as Windows Vista and others. It provides a comprehensive insight and pragmatic advice on the process of building secure Web-based applications and makes recommendations on how to best address security threats.

Information security and related control considerations have always been important organization issues. Electronic financial reports and online e-commerce creates considerable security concerns. Viruses, worms, and hackers put online e-commerce businesses at particular risk. A secure information system is vital to publicly traded companies' operations and the financial reporting process. As security breaches become more prevalent in business environments, companies should consider the appropriate security technologies that help prevent, detect, and correct cybercrime, including electronic financial statement fraud. Security technologies and related safeguarding controls should be designed and implemented. Examples of these security technologies intended to protect information systems and the electronic transfer of information are electronic authorization, electronic authentication, and encryption.

Control considerations for the electronic financial reporting process are security services, antivirus solutions, firewalls, encryption technologies, and intrusion detection. An information security service provides security management, firewall integration, and vulnerability assessments. Security programs, including antivirus software, detect and prevent computer viruses that damage information systems. An effective firewall protects computer systems from hackers on the Web.

Encryption technologies provide solutions to access controls while intrusion detection alerts companies to hacking and other unauthorized attempts to access their systems. Data integrity and confidentiality are two major elements stressed in security concerns. Data integrity can be enforced through hash totals, while data confidentiality can be enforced through cryptography and encryption. XBRL developers have not yet properly addressed these security measures, primarily because XBRL was developed under the premise that data integrity can be improved by taking such measures as supplementary redundant error correction bytes, cryptographic hashing, and signing with a private key.

Security of the XBRL-based financial reporting process is a major challenge for publicly traded companies to ensure that access to electronic data is restricted to authorized personnel and that modifications and destruction of electronic data are restricted to appropriate individuals. Companies should design and implement adequate and effective control activities to safeguard electronically presented financial information from hackers and potential manipulation. Security is an issue that may plague XBRL primarily because many organizations may not be comfortable using a system that transmits financial information so easily and exposes it to the risk of hackers breaking into their system. Companies can protect the integrity of their XBRL-based financial system and ensure its security by using any of the available Internet security programs, such as SysTrust and WebTrust offered by the American Institute of Certified Public Accountants (AICPA).

Cell Phones as Banks

In the Philippines, the cell phone market is unique. Thirty-five percent of the population has cells phones and 95 percent of the remaining population has access to cell phones through a friend or relative. SMART Padala is a mobile-phone-based cash remittance system. This system can be used to move money into and out of cell phone–based bank accounts. In the Philippines, people can then use money on their cell phones at the local McDonald's to pay for a Big Mac, fries, and a Coke. This same technology can be used by drug dealers and their customers to transfer cash. More important, cell phone cash transfer technology and other Internet-based extratraditional money systems such as e-Gold and the Electronic Wallet are the methods of choice for international money launderers from organized crime, drug traffickers, to terrorist organizations.

FUTURE OF XBRL

Under XBRL, an electronically readable tag (bar code) is assigned to each financial statement item, which provides additional context, including definition of the item, accounting standards used, time period, and company. These electronic tags are standardized, are defined according to commonly accepted taxonomies, and remain unchanged when they move from one computer platform to another. They are accompanied by a tagging tool that retrieves the tags from the standard taxonomies and applies them to the software being used (e.g., Excel, Microsoft Word).

XBRL makes it easier to generate, compile, validate, and analyze business and financial information. These features of XBRL improve the quality, completeness, comparability, and timeliness of business and financial information in making decisions. XBRL has developed an international public consortium of about 550 organizations from 20 countries worldwide. More than 8,200 financial institutions in the United States have submitted their quarterly call reports, also known as risk-oriented filings, in XBRL format, to federal banking regulators since the fall of 2005. Institutions have substantially reduced their filing compliance costs and provided higher-quality data and better analytical procedures (ratios) and more relevant benchmarking data. In additions, about 25 public companies (e.g., Ford, General Electric, Microsoft, PepsiCo, Bristol-Myers Squibb, and United Technologies) have filed their annual (10-K) and quarterly (10-Q) reports in XBRL as part of a voluntary SEC pilot program. Other countries (e.g., Australia, Canada, China, the European Union, India, Japan) are following suit.

On January 30, 2009, the SEC adopted rules that would require companies to provide to the Commission financial statements in XBRL format, as well as posting to corporate Web sites (if companies maintain Web sites). These rules will apply to domestic and foreign companies using U.S. GAAP and to foreign private issuers using International Financial Reporting Standards as issued by the International Accounting Standards Board. These rules are effective April 13, 2009.[9] By June 15, 2010, all domestic and foreign large accelerated fillers that use U.S. GAAP will be subject to interactive data reporting, while by June 15, 2011, all remaining companies will have to fulfill the requirements and report using XBRL format.[10] Its use will make it easier for public companies to file their 10-Ks and 10-Qs with greater flexibility in reporting. Potential high interactive data convergence costs and possible interruption in the filing process, and particularly initial abuse and fraud, should be evaluated. The average cost of first submission with block-text footnotes and schedules was established as $40,510 and could go as high as $82,220 with additional 36 to 38 months for XBLR preparation.[11] Auditing firms should start preparing to provide assurance on the quality of XBLR financial statements.

Scope

The scope of the audit function can be increased by use of the XBRL format. Auditors are no longer limited to sample tests and assessing the sample results as they relate to the transaction population. Highly automated audit procedures (e.g., data mining, also called data extraction and analysis) can be used to gather and analyze sufficient and competent audit evidence. Auditors should perform continuous audit procedures, particularly when the audit process has identified anomalies. Auditors should ensure that their organization’s Web site, when displaying financial information, properly indicates when, where, and how the information is hyperlinked to matters outside of financial statements. To be effective, auditors will need to use a targeted approach; otherwise, the number of apparently anomalous transactions may overwhelm them.

Continuous Assurance

The technological advances of the Internet have drastically changed the traditional means of preparing and disseminating business information. Currently, many companies publish their business information, including both financial information (e.g., audited financial statements and the independent auditor's report, Forms 10-K and 10-Q) and other information (e.g., management analyses, marketing) electronically. The electronically published business information is highly integrated through hyperlinks (e.g., pension accounting policies and practices can be connected with personnel promotion and advancement plans). This makes separation of financial information from other information difficult if not impossible and thus has raised several concerns for independent auditors. These concerns and questions have been addressed in "Practice Alert 97-1" by the SEC Practice Section Professional Issue Task Force.[12] The Practice Alert raises three questions:

1. What is (are) an independent auditor's obligation(s) for other information presented in an electronic site that contains audited financial statements and the related auditor's report?

   The Interpretation to Auditing Standards of the AICPA pertaining to "other information in electronic sites that contain audited financial statements" addressed this question. The interpretation advises that independent auditors do not have an obligation to read or consider other information included in an electronic site.

2. How may a client ensure the security of information integrity when published on the Internet?

   The independent auditor should discuss the security and related control activities of electronic sites with the client to ensure integrity of these sites.

3. Can a client who presents audited financial statements and other information on the Internet set it up so that users know when they are hyperlinking to matters outside of audited financial statements?

   Auditors should advise their clients to create distinct boundaries around their audited financial statements and related audit reports and to remind users of this. Alternatively, entities may wish to clearly mark each page of the audited financial statements and related audit report as being part of the annual report. Entities may also wish to provide an embedded link to their electronic site that would allow easy and complete access to all parts of audited financial statements and the related audit report in an orderly manner.

The challenge for auditors is to keep assurance on the data up to date, especially when financial information is prepared in online, real-time, XBRL-based format. Continuous auditing can be achieved only by embedding source code into the organization's reporting system that reports abnormalities to auditors for immediate review. Shorter time frames for reporting financial information would result in the need for a high degree of reliable automation in producing information soon after the occurrence of events.

Continuous auditing allows auditors to specify transaction selection criteria to choose the specified transactions and perform tests of controls and substantive tests throughout the year on an ongoing basis. Thus, auditors should be able to examine the design of the XBRL-based accounting system and insert the required audit modules in the process and outputs. Continuous auditing gathers audit evidence regarding five audit questions:

1. How data are electronically gathered?
2. How, where, why, and from what parties did the data originate?
3. What authentication techniques are used?
4. What networks are used to originate and transmit the data?
5. How are the data processed once they are received by the XBRL system?

Auditors also use control agents, which are auditor-defined heuristics applied to a transaction set.[13] The agent, upon finding unusual activities, first searches for similar activities to explain the activity pattern and alert the auditor regarding unprecedented or unusual activities. Continuous auditing assists auditors in shifting from a reactive to a proactive audit model. XBRL enables auditors to move from a paper-based conventional audit to an electronic-based continuous assurance.

In the electronic environment, the focus of audit shifts from manual detection of financial statement fraud to technology-based prevention and detection of financial statement fraud. Although some financial statement fraud may never be prevented, the use of audit software packages can assist auditors to build in reports and analysis to identify areas of concern when unusual relationships exist. The ability to include internal checks into advance computer systems can enable management and auditors to prevent and detect errors and irregularities that can cause financial statement fraud. The use of technological advances, such as computerized audit tools and techniques (CATTs), enables auditors to test almost 100 percent of transactions, which in turn enable them to discover financial statement fraud more frequently, effectively, and efficiently.

Fair Disclosure

XBRL does not require any further disclosure of financial information beyond what is currently required under the generally accepted accounting principles (GAAP). XBRL is a GAAP-neutral tagging structure, using a GAAP-specific language to describe financial information by industry sector. XBRL is intended to be used on a global basis by creating tagging data specifications that conform to the various countries' accounting principles and industry practices. XBRL, which enhances the capability of financial reports, enables flexibility to accommodate a company's internal environment, processes, systems, and styles. XBRL enables organizations to comply with the new SEC Fair Disclosure regulation by electronically and simultaneously disclosing all relevant financial information to all users of financial reports,

including analysts and investors. This online and real-time disclosure of financial information creates a level playing field for all users of financial statements and thereby reduces the likelihood of selective disclosure and inside trading. Thus, XBRL, while not requiring additional disclosure beyond what organizations currently are presenting, can aid in addressing the new SEC Fair Disclosure regulation with the XBRL format. All parties involved in the business reporting chain will have equal and simultaneous access to publicly available information disseminated by corporations.

Privacy

XBRL is derived from XML, which tags financial information. The tagged information is then accessible to a wide variety of users for different purposes across all programs. As the number of XBRL users worldwide increases, more financial information is captured, stored, and made available electronically. The power of XBRL enables financial information to be tracked, used, and interpreted without the organization's consent or knowledge. XBRL adds a new direction to the online privacy consideration. The *privacy of information* refers to security and confidentiality of personal and financial information obtained by businesses about their customers or trading partners. This privacy of information has not been properly safeguarded and, in many instances, has been violated. Three examples of e-commerce security lapses are:

1. America Online's (AOL) admission in July 2000 that hackers gained access to member accounts through an e-mail virus sent to its employees
2. Lawsuits brought against AOL's Netscape division accusing it of breaking federal privacy laws by tracking customer downloads
3. Confession by a member of failed consumer-oriented dot-coms that they sold customers' personal information to the highest bidder

Another example of the privacy-related issue is toysmart.com, which went bankrupt and attempted to sell off an extensive customer database as part of its bankruptcy liquidation efforts. The Federal Trade Commission (FTC) ruled that ''even failing dotcoms must abide by their promise to protect the privacy rights of their customers,'' primarily because the company had a posted privacy policy stating that the company would not sell data to third parties.[14]

These incidents of violation and lack of security of customer information have raised several consumer personal and financial privacy issues:

- Should businesses establish and maintain adequate and effective privacy policies and systems?
- What information can be gathered and stored by such systems?
- Should the gathered information be used by the businesses?
- Can businesses share or sell customers' information without their permission?

- Can customers verify, change, and/or delete the information?
- Should there be an independent verification of the established privacy policies and systems?
- Should the use of cookies be allowed?
- Is there a need for legislation to protect online consumers' privacy?

Trust

XBRL can produce and disseminate a significant amount of business information. The accuracy and reliability of distributed information can play an important role in the success of XBRL as a business-reporting vehicle. The accounting profession, especially the AICPA by establishing WebTrust standards for practitioners who perform such services for their clients, can provide reasonable assurance on the trustworthiness of XBRL-generated business reports. To obtain customers' confidence regarding the proper stewardship of their personal and financial privacy, many businesses, especially dot-coms, have obtained seals or insignias for their Web sites. Many organizations have offered seals for businesses that maintain adequate and effective privacy policies for their Web sites.

Effective and efficient privacy seal programs provide reasonable assurance that organizations' (1) privacy policies for the collection, use, and disclosure of identifiable personal information are adequate, (2) privacy practices are in compliance with stated policies, and (3) consumers' complaints are resolved properly and in a timely manner. Several privacy seal programs have been created. These programs serve eight purposes:

1. Protect individually identifiable information
2. Set standards for ethical e-commerce
3. Satisfy guidelines for self-regulation
4. Foster consumer confidence in the way businesses handle personal information online
5. Guarantee that organizations safeguard the collected personal information
6. Promote self-regulation of e-commerce by protecting online privacy
7. Provide a mechanism for consumer-friendly dispute resolution
8. Require participating organizations to conduct annual assessments of their privacy policies and practices

XBRL Implementation

Corporations should cooperate with software developers and Web site designers in further development of software components to establish XBRL-compatible code and to apply XBRL to a variety of software programs. Corporations should

effectively and efficiently implement XBRL to take advantage of a broad range of XBRL benefits, including the improved reliability and flexibility of financial reports and possibility of continuous assurance. Proper implementation of XBRL requires:

- Development of taxonomy (specification) that is standardized and uniform among all companies in the same industry
- An application that enables the preparation of financial statements ''tagged'' with the XML-based format adhering to the specification
- Style sheets that render information for a specific format or variety of formats

ANTIFRAUD APPLICATIONS FOR PRACTICE

Information technology and the digital environment play a role in fraud and computer crimes due to these factors:[15]

- Increased use of information technology in business
- Businesses centered on technology, including Dell, IBM, Google, eBay, and Microsoft, to name a few
- Increased data use by financial statement auditors, fraud auditors, and forensic accountants
- Increased exploitation of information technology by fraudsters and cybercriminals

In fulfilling their fiduciary responsibilities, corporate governance professionals need to ensure that the organization's digital environment is adequately protected. They must ensure that:

- The electronic information feeding the financial reporting process is timely and accurate.
- Reasonable information technology protections exist to support organizational viability and vitality given a digital world and its associated threats and opportunities.

CYBERFORENSICS

The increased role of IT in fraud and cybercrime results in a corresponding increase in the need for organizational professionals with digital knowledge, skills, and abilities, not just in operational systems but also in fraud, computer crime, and cybercrime. Evidence about who, what, where, when, and how often exists in digital form, in some cases exclusively. Further, most state-of-the-art digital forensics tools and techniques have come into existence in the last 10 to 20 years. The

pervasiveness of digital media and information in virtually every aspect of an organization's life illustrate the increased need for cyberforensic specialists. Cyberforensics involves the capture, preservation, identification, extraction, analysis, documentation, and case preparation related to digital data and events. Some sources of digital evidence that the nontechnically savvy professional may not be aware of include:

- Digital "fingerprints" in metadata, e-mail headers, and electronic cookies
- Hidden data located on storage devices
- The ability to recover deleted files
- Data located in unused space, temporary files, random access memory (RAM), and various logs
- The possibility of retrieving data that was overwritten with new data

INFORMATION SYSTEMS GOVERNANCE AND CONTROLS

Information systems governance and controls are concerned with the prevention, deterrence, and detection of bad acts in a digital environment. An organization's IT group must adhere to governance best practices consistent with those of the organization as a whole. The Information Systems Audit and Control Association (ISACA) is a global organization for information governance, control, security, and audit, and its information systems auditing and control standards are followed by practitioners worldwide. ISACA defines IT governance as a set of principles to assist enterprise leaders in their responsibility to ensure that the organization's IT needs are aligned with the business and deliver value, its performance is measured, its resources are properly allocated, and its risks are mitigated. The best practices associated with IT governance should include preventive countermeasures against fraud and cybercrime. Continuous auditing and proactive fraud auditing are typically associated with antifraud best practices.

Risk assessment is a critical aspect of good corporate governance, and the same concept is applicable in an information technology environment. An IT risk assessment should identify risks associated with the digital environment. That assessment requires that IT leadership know and understand how IT prevents and detects internal and external attack, including those associated with the commission of frauds and computer and cybercrimes. As part of that risk assessment, IT professionals need to identify and understand the ways in which IT systems typically are exploited during fraud acts and cybercrime, how IT systems are used to facilitate fraud concealment, and how IT security is commonly breached or circumvented.

DIGITAL EVIDENCE

Electronic information capture is the first step in the investigation of digital evidence; however, it is possible to hinder a successful legal outcome if one does

not follow the best practices and the legal requirements associated with digital capture. A successful cyberforensics investigation requires a professional who has the technical background in computer technology and systems and is familiar with the relevant rules of the legal system and investigations. For example, the simple act of turning on a confiscated computer can make all the evidence on that computer inadmissible in a courtroom environment because turning on the computer alters the hard drive and thus the chain of custody is broken. Only those persons with specialized training, experience, and appropriate professional certifications should initially capture digital evidence.

The sources of digital evidence are evolving and expanding but include cell phones, personal digital assistants (PDAs), BlackBerries and similar phones, trinkets with digital storage (e.g., watches, USB pens, digital cameras), jump drives, media cards, e-mail, voice mail, CDs, DVDs, printer memory, RAM, slack space, removable drives, and iPod/MP3 players and radio players. There are also the conventional sources such as laptops, office computers, home computers and external drives, servers on the Internet (e.g., e-mail messages), and the entity's own servers. Special software and hardware tools are available to capture digital evidence, such as SF-5000, RoadMASSter, and write blockers.

DETECTION AND INVESTIGATION

Notwithstanding the utilization of traditional detection and investigation techniques applied in a digital environment, some additional tools and techniques are also important. Those tools and techniques include data mining software, which is useful for data extraction and analysis, and continuous monitoring and auditing software. Most data extraction and analysis tools can retrieve, filter, extract, sort, and analyze data from accounting databases as well as identify gaps, duplicates, missing information, and statistical anomalies.

CYBERCRIME

The Department of Justice defines cybercrime as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution. Cybercrime knowledge, skills, and abilities include a basic understanding of the types of crimes as well as special laws and relevant criminal code. Some typical cybercrimes are outlined in Exhibit 13.3.

Exhibit 13.3 Sample of Types of Cybercrimes

Unauthorized computer intrusion	Hacking	Infrastructure attacks
Digital credit card theft	Online/e-mail extortion	Viruses, worms, etc.
Identity theft	Online gambling	Theft of computers
Online narcotic sales	Cyber-terrorism	Telecommunications fraud

The last thought:

> *Fraud is not committed by accounting systems or computers. It is carried out by living, breathing human beings who outwardly seem no different from you and me.*
>
> —Joseph Wells, founder and chairman of the Association of Certified Fraud Examiners

NOTES

1. Allison Diaz, "Meet A-Z: The Computer Hacker behind a Cybercrime Wave," *USA TODAY*, August 5, 2008.
2. Ibid.
3. The discussion of NetWar is largely attributed to John Arquilla and David Ronfeldt, "The Advent of NetWar," first edition, RAND Corporation (August 6, 1996).
4. The concept of legitimate global business operating in more networked form was described extensively in Thomas Friedman's *The World Is Flat* (Farrar, Straus and Giroux, 2006).
5. G. S. Smith, "New Age Technology Threats and Vulnerabilities," *Journal of Forensic Accounting* 2 (2001): 125–130.
6. A. Ruppeport, "SEC Maps Interactive Filing Mandate," May 14, 2008; available at cfo.com.
7. *American Banker* (1999); available at www.americanbanker.com.
8. Ibid.
9. American Institute of Certified Public Accountants. XBRL resources; available at www.aicpa.org/Professional+Resources/Accounting+and+Auditing/BRAAS/XBRL.html#XBRL
10. SEC. Final Rule 17 CFR Parts 229, 230, 232, 239, 240 and 249 Interactive Data to Improve Financial Reporting (April 13, 2009); available at www.sec.gov/rules/final/2009/33-9002.pdf.
11. Ibid.
12. AICPA, "Practice Alert 97-1," *CPA Letter* (January/February 1997); available at www.aicpa.org/pubs/cpaltr/Jan 97/suppl/prac.htm.
13. A. Kogan, F. Sudit, and M. Vasarhelyi, "Some Auditing Implications of Internet Technology" (1999); available at www.rutgers.edu/accounting/raw/mikles/tcon3.htm.
14. B. Fonseca, "Blanket Insecurity? Web Security, Privacy Problems Raise Confidence Issues," *InfoWorld,* July 10, 2000, 1.
15. This section was derived primarily from the NIJ manuscript, "Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students." It is available from the NIJ Web site at www.ncjrs.gov/pdffiles1/nij/grants/217589.pdf.

Chapter 14

Fraud Examination Practice, Education, and Research

INTRODUCTION

Is financial reporting fraud or other malfeasance involved in the financial markets meltdown of 2008 that led to the $1 trillion bailout of Wall Street by the U.S. government? As of September 2008, the Federal Bureau of Investigation (FBI) announced that it had opened investigations of four mortgage giants: Fannie Mae, Freddie Mac, Lehman Brothers Holding Company, and the insurer American International Group (AIG), Inc.[1] In total, the FBI disclosed that 26 corporations were under investigation as part of the bureau's mortgage fraud inquiry. In addition, 1,400 individual real estate lenders, brokers, and appraisers were being investigated. While the investigations will take time, the FBI plans to go where the evidence and facts lead.[2]

The 2008 global economic meltdown, coupled with international competition, corporate misconduct, and a litigious business environment, has made the global economy and business more vulnerable to corruption, abuse, and fraud. During the past decade, the revelation of numerous cases of financial statement fraud and other financial malfeasance has caused the business community and the accounting profession to become increasingly concerned about responsible corporate governance and reliable financial reporting. These issues have brought the topics of fraud examination and forensic accounting to the forefront, not just because of the need to investigate malfeasance but also because of the efforts of professionals related to antifraud measures, tools, and techniques.

Fraud examination applies business, accounting, auditing, and legal concepts to facts or hypotheses under consideration as well as antifraud efforts. Forensic accounting is the intersection of accounting and the law and includes litigation support consulting, expert witnessing, and the resolution of fraud allegations. Recently, fraud examination and forensic accounting have received considerable attention from the business community, accounting profession, and experts from related fields such and intelligence and interviewing. Importantly, fraud examination and forensic accounting also interact with professionals from the law, criminology, sociology, psychology, intelligence, computer forensics, and other forensic sciences.

THE INTERRELATIONSHIP: AUDITING, FRAUD EXAMINATION, AND FORENSIC ACCOUNTING

Exhibit 14.1 shows how the knowledge and skills of auditing, fraud examination, and forensic accounting interrelate. Traditional auditing procedures address fraud to the extent that Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit,* and other auditing requirements necessitate a search for fraud; however, auditors have no responsibility to plan and perform auditing procedures to detect misstatements that are not judged to be material (whether caused by error or fraud). Corporate management also has increased responsibility to design and implement internal controls to prevent and detect fraud as a result of the Sarbanes-Oxley Act (SOX). Allegations of fraud are often resolved through court action, which illustrates the overlap between fraud examination and forensic accounting. However, each also encompasses activities unrelated to the other; for example, fraud professionals often assist in fraud prevention and deterrence efforts that do not directly interface with the legal system, while forensic accountants work with damage claims, valuations, and legal and other issues that do not involve allegations of fraud.

The interrelationship among auditing, fraud examination, and forensic accounting is dynamic, changing over time due to political, legal, social, and cultural

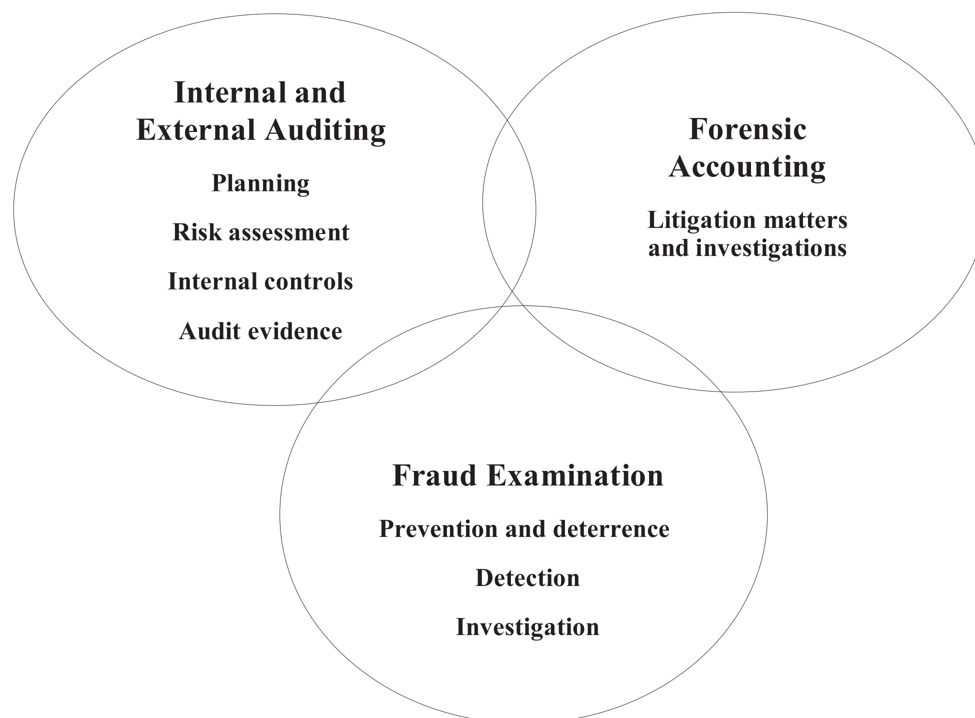


Exhibit 14.1 The Interrelationship: Auditing, Fraud Examination, and Forensic Accounting

events. In addition, the level of overlap between forensic accounting and fraud examination may be larger than depicted here. Because external auditors operate in an environment impacted by SAS No. 99 and SOX, they are expected to have, at a minimum, adequate knowledge and skills to ensure that the financial reports are free from material fraud.

FORENSIC ACCOUNTING PRACTICE

LITIGATION SUPPORT CONSULTING

Litigation support consulting activities consist of assisting lawyers to (1) assess the usefulness, reliability, and relevance of financial information, (2) gather financial data, (3) prepare questions for depositions, and (4) conduct interrogations. The field of litigation consulting expanded rapidly during the past decade. Epstein and Spalding report seven activities on which accounting experts commonly consult:

1. Product liability
2. Commercial contract claims
3. Patent, trademark, and copyright infringement
4. Mergers and acquisitions
5. Insurance claims
6. Reorganization and bankruptcy
7. Toxic tort claims[3]

Litigation consultants help lawyers in the areas of financial information review, analysis, and interpretation. Financial information analysis and interpretation is the process of determining the relevancy, usefulness, and reliability of information presented for a legal action. Financial statement analysis assesses financial information presented to the court and assists attorneys in interpreting the findings. Plaintiff and defense attorneys use financial information detection and analysis in the discovery stage of their own cases in order to prepare for the opposing litigation team's testimony. The forensic accountant's financial knowledge and expertise can be useful to attorneys because they often lack adequate financial knowledge and expertise to effectively represent their clients with forensic accounting support.

EXPERT WITNESSING

Fraud examiners and forensic accountants often serve as expert witnesses. Judges qualify expert witnesses based on their special knowledge, skill, experience, and training to assist jurors in reaching conclusions of fact in areas beyond their ordinary experience and comprehension. Business forensic professionals often are recognized as expert witnesses by judges during judicial proceedings. Accountants

and other forensics professionals serving as expert witnesses must form their opinions objectively and independently and often must use layman's language to simplify technical jargon. As an expert witness, the accountant can help explain or interpret complex accounting or financial data that otherwise might not be understood. Experts often are utilized in complex financial cases because they are able to explain accounting jargon in lay terms for judges and jury and can give an opinion on and draw conclusions from hypothetical situations on the witness stand. Fraud examiners and forensic accountants serving as expert witnesses can assist attorneys in gathering relevant information, educating them regarding the technical aspects of the case, and providing expert testimony.

Communication skills, presentation style, and self-control are required traits for an expert witness. As an expert witness, professionals should be aware of the potential dangers of an adversarial environment and attempt to be objective while there is great pressure from the attorney to be partisan. Epstein and Spalding point out: ''As an expert witness the CPA presents opinions publicly in an objective fashion, but as a consultant the CPA advises and assists the attorney or client in private. In the private role, the CPA provides assistance more like that of an advocate to help the attorney identify case strengths and weaknesses or to develop strategy against the opposition.''[4]

Does Doing the Right Thing Pay Off?

From the notorious financial reporting frauds of the early 2000s through the subprime mortgage crisis and related global financial markets meltdown, we have seen the wealth of investors decimated through fraud, malfeasance, corruption, abuse, incompetence, and neglect. In response, one solution is to focus on improved corporate governance. A basic question remains: While research suggests that best practices regarding corporate governance avoids losses, does doing the right thing have a positive effect?

Trying to measure an elusive concept such as ''doing the right thing'' is a challenge, to say the least. Nevertheless, three researchers—Baruch Lev, Christine Petrovits, and Sresh Radhakrishnan—proxied this concept by examining charitable giving. Their study examines the impact of corporate philanthropy growth on sales growth using a large sample of charitable contributions made by U.S. public companies. The researchers found that charitable contributions are significantly associated with future revenue. The results are particularly pronounced for firms that are highly sensitive to consumer perception, where individual consumers are predominant, such as retailers and financial services. In addition, a positive relationship was observed between contributions and customer satisfaction. Overall, their evidence suggests that corporate philanthropy, under certain circumstances, furthers economic objectives of firms.

These results were further documented by Herb Greenberg. He interviewed Michael Castine, president of Dover Management, who observes that the ''Philosophy from top management filters throughout the organization.'' If a company is known for its philanthropy, Castine says, ''It's an indicator of cash on its balance sheet. If there's a

(*continued*)

problem, the first thing to go is the philanthropic contributions.'' Dover's research suggests that companies with a good relationship between philanthropy and operating earnings have outperformed the broader Standard & Poor's 500 index by 3.5 percentage points a year over a five-year period.

Dover Management argues that philanthropy is like paying dividends: ''You need to have significant free cash flow and the confidence that you're going to continue to have that.'' Greenberg observes that companies such as Avon Products, Pfizer, and Nike are examples of organizations that have a strong charitable bent. Nike's financial performance has been consistently strong; Pfizer and Avon, less so. However, all three boast exceptionally strong free cash flows. Dover Management favorites include PepsiCo, Johnson & Johnson, and Kimberly-Clark Corp.

Sources: Baruch Lev, Christine Petrovits, and Suresh Radhakrishnan, ''Is Doing Good Good for You? How Corporate Charitable Contributions Enhance Revenue Growth,'' SSRN Working Paper Series, September 1, 2008. Herb Greenberg, ''How Doing the Right Thing Pays Off,'' MarketWatch, October 28, 2007.

FRAUD EXAMINATION

Fraud examination is the practice of rigorous data detection and analysis with a built-in suspicion and skepticism that fraud and violations of applicable laws, rules, and regulations are always possible. It applies to business, accounting, and legal principles, rules, and investigative techniques to financial and legal issues under investigation. Fraud examiners strengthen the financial reporting process by (1) assisting in the deterrence, detection, and reporting of financial statement and occupational fraud, including investment fraud, kickbacks and commercial bribery, bank fraud, credit card fraud, electronic funds transfer fraud, and computer fraud and (2) conducting fraud vulnerability assessments and designing antifraud policies, procedures, and controls.

Fraud examination involves the investigation of financial and other documentation for the criminal activity of fraud. While financial auditing often focuses on detecting material misstatements in financial statements, whether caused by errors or fraud, fraud investigation also concentrates on smaller errors, irregularities, or frauds that are below the materiality threshold and thus can be below the radar of the external auditor. These small misstatements can indicate potentially large problems with the accounting system. According to Bologna and Lindquist, fraud examiners should determine when (1) transactions seem ''odd'' as to when they occur; their frequency, place, or amount; or the parties to which they relate, (2) internal controls are overridden, and (3) chronically low employee motivation and morale occur.[5] Fraud investigators use their knowledge, training, skills, expertise, and intuition to gather evidence to demonstrate beyond a reasonable doubt that fraud has occurred.

Interviewing and interrogating are two essential activities that fraud examiners typically perform. Interviews usually are conducted earlier in the investigative process to obtain relevant information as to the facts and issues regarding the potential fraudulent incident. Interrogation often is reserved for suspected perpetrators to elicit voluntary confessions from them. Fraud investigators should not only ask the right questions but also carefully listen to the responses and observe the body language of the individual being questioned. Fraud investigators should recognize that most fraud cases would eventually end with litigation. Thus, they should be very skeptical and conduct each fraud investigation with the notion that:

- Fraud must be proven beyond a reasonable doubt
- Evidence gathered must be competent, sufficient, persuasive, and convincing
- Investigation must be conducted in a legal manner
- Documentation must be adequate
- Confession must be voluntary

Fraud examination and forensic accounting are becoming appealing specialization opportunities for accountants, auditors, and law enforcement and professionals from related fields. Several reports and studies:

- Indicate that the public and business community are becoming more concerned with excessive fraudulent financial activities
- Suggest that the accounting profession provide guidance on the consideration of fraud in conducting a financial statement audit
- Call for the promotion of fraud examination practices and education[6]

To be a successful fraud investigator, professionals should be effective examiners, skeptical auditors, and designated professionals. The professional designation for fraud examiners is the Certified Fraud Examiner (CFE). The CFE designation is sponsored by the Association of Certified Fraud Examiners (ACFE) and described in the next section.

CERTIFIED FRAUD EXAMINER

According to the results of a 2008 survey conducted by the American Institute of Certified Public Accountants (AICPA), the demand for Certified Public Accountants (CPAs) providing forensic accounting has accelerated. Sixty-eight percent of the 5,400 members of the AICPA's Forensic Valuation Services Section who were polled in 2008 say their forensic practices have expanded over the past year. Of those respondents who stated increased demand, 67 percent cited computation of economic damages as the leading reason, followed by marital disputes (56 percent) and investigations of financial statement fraud (54 percent).[7]

The CFE designation is an excellent credential for fraud examiners, forensic accountants, and law enforcement to possess. The CFE is administered by the Association of Certified Fraud Examiners (formerly the National Association of Certified Fraud Examiners), which was established in 1988.[8] The membership, as of 2008, is over 40,000 members who are certified and trained in various aspects of detecting, investigating, and preventing occupational and financial statement fraud as well as white-collar crimes. Members are scattered across 70 countries and have organized local chapters. The association was established (at least in part) to respond to the Treadway Commission Report, which established recommendations to reduce the incidence of fraud, and CFEs have investigated more than 1 million alleged cases of civil and criminal fraud.

The mission of the ACFE is to reduce the occurrence of fraud and white-collar crime by assisting its members to prevent, detect, investigate, and remediate such occurrences. To fulfill this mission, the ACFE:

- Provides bona fide qualifications for CFEs through a uniform examination
- Sets high standards of admission through demonstrated competence and continuing professional education
- Requires and monitors adherence to a strict code of ethics
- Serves as an international representative for CFEs to business and government
- Promotes the public's confidence in the integrity, objectivity, and professionalism of CFEs

The CFE program is an accrediting process established for individuals who have the specialized skills to detect, investigate, and deter fraud. The CFE designation provides an upper hand to those who wish to practice in the field of fraud investigation. Those who possess the CFE designation will be better prepared to ride the wave of forensic accounting and related specializations. Six specific benefits provided through membership and possession of the designation include:

1. Professional recognition within the accounting profession and the business community
2. Career opportunities within the expanding service industry of forensic accounting including fraud investigation
3. Membership in a local chapter that will allow for the communication of ideas and the discussion of issues relevant to the forensic accountant
4. Professional training that will assist the CFE in maintaining current knowledge as well as preparing them for future expertise
5. Publication and periodicals that are designed to keep the CFE informed on current and emerging issues within and related to the profession
6. Continuing education to keep abreast of current developments in the area of forensic accounting

The ACFE has also made significant contributions to efforts of academics at colleges and universities through its higher education initiative, the creation of the Institute for Fraud Prevention, and other efforts.

CERTIFICATION IN FINANCIAL FORENSICS

In May 2008, the AICPA's governing Council authorized the creation of a new CPA specialty credential in forensic accounting. The credential, Certification in Financial Forensics (CFF), combines specialized forensic accounting expertise with the core knowledge and skills that make CPAs among the most trusted business advisors. The CFF encompasses fundamental and specialized forensic accounting skills that CPA practitioners apply in a variety of service areas, including:

- Bankruptcy and insolvency
- Computer forensics
- Economic damages
- Family law
- Fraud investigations
- Litigation support
- Stakeholder disputes
- Valuations

To qualify, a CPA must be an AICPA member in good standing, have at least five years of experience in practicing accounting, and meet minimum requirements in relevant business experience and continuing professional education. In the future, the AICPA plans to add an examination requirement as part of the process to award the CFF.

TRAINING COMPETENT AND ETHICAL FRAUD EXAMINERS AND FORENSIC ACCOUNTANTS

The accounting profession, business schools, accounting programs, public accounting firms of all sizes (Big Four and non–Big Four), law enforcement, and academics and professionals from related fields have demonstrated a keen focus on antifraud and forensic accounting training and education. Next are listed eight ways to ensure training competent and ethical forensic accountants:

1. Integrate forensic accounting, corporate governance, and ethics into the academics programs.

2. Make internships a part of the education process. Hands-on and practical experience is important in exposing students to professional issues retaining to fraud examination and forensic accounting.
3. Encourage accounting students to obtain their CFE, CFF, and other professional certifications [CPA, Certified Management accountants (CMA), Certified Internal Auditors (CIA), Certified Government Financial Management (CGFM)].
4. Ensure that the professional exams adequately and effectively test standards, knowledge, skills, competency, and integrity derived from antifraud education, training, and experience.
5. Require antifraud education to obtain professional certifications and licenses.
6. Establish diversified and strong advisory boards to oversee and support academic programs.
7. Promote professional organizations [Beta Gamma Sigma, Beta Alpha Psi, Institute of Management Accountants (IMA), Institute of Internal Auditors (IIA), Associations of Certified Fraud Examiners (ACFE) students' chapters].
8. Promote effective master's and doctoral programs (business administration, DBA; philosophy, PhD) with emphasis and concentration in fraud examination, forensic accounting, and financial forensics.

The Treasury Department's Advisory Committee on the Auditing Profession released its report specifying recommendations for improving the profession. Among recommendations for business schools and accounting programs, the committee suggests implementation of market-driven curriculum that continuously evolves to meet the emerging needs of the auditing profession and strengthening the diversity (minorities, gender, ethnic) in the auditing profession. The committee recommends improving audit firm's fraud prevention and detection skills as well as its communication with investors regarding its fraud detection responsibilities. The committee recommends that the Securities and Exchange Commission and Public Company Accounting Oversight Board require auditors of public companies to clarify in their audit report their role in detecting financial statement fraud.

To improve objectivity, independence, and vibrancy of public company auditing firms, the committee recommends:

- Reducing the barriers to growth of smaller auditing firms
- Disclosure of annual financial statements by auditing firms
- Adoption of annual shareholder ratification of auditors
- Monitoring potential sources of catastrophic risk faced by auditing firms
- Designing a mechanism for the preservation and rehabilitation of troubled large public company auditing firms

FRAUD EXAMINATION AND FORENSIC ACCOUNTING EDUCATION

Society expects auditors, accountants, law enforcement, and related professionals to assume more responsibility for ensuring the integrity, quality, and reliability of financial reporting. To improve audit effectiveness, the Public Oversight Board[9] suggests forensic-type phase to be included in audit fieldwork. The extent of knowledge required for fraud examiners and financial forensic professionals in conducting fraud investigation, performing litigation services, and giving expert testimony is extensive and should have a prominent position in the higher education curriculums. According to Rezaee, Reinstein, and Lander,[10] forensic accounting education traditionally has been limited to continuing professional education sessions for practicing accountants; only a few universities teach forensic accounting; and auditing textbooks do not provide sufficient coverage of fraud examination. The majority of academicians and practitioners who responded to a survey conducted by Rezaee and Burton[11] (about 75 percent) indicated that demand for forensic accounting (fraud examination) has increased and will continue to increase. Given the demand for fraud examination practice and education, college/university programs should provide forensic accounting and financial forensics education.

Individuals seeking to enter the specialized field of antifraud efforts, forensic accounting, and financial forensics, as well as employers hiring these entry-level professionals, have urged educational institutions to enhance their coverage of fraud, forensic accounting, and financial forensics in their academic programs. In response, the National Institute of Justice (NIJ), the research, development, and evaluation agency of the U.S. Department of Justice, supported a project to develop a model curriculum for fraud and forensic accounting education. The NIJ manuscript is titled "Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students" and is available from the NIJ Web site.[12] As described in the document, the NIJ model curriculum was created in concert with 46 subject matter experts (the technical working group) from across the nation, representing corporate and industry stakeholders, professional services providers, law enforcement, the legal community, government and regulatory stakeholders, professional organizations, and academics. The project was designed to develop model curriculum guidelines for educators, students, and employers to understand the knowledge, skills, and abilities necessary for success in this growing field. This curriculum was the result of the collective input from the subject matter experts and was tested in classrooms. Therefore, these guidelines were developed with the intention to serve the academic and professional communities' need to better understand the knowledge and skills required of those entering this field and to assist them in developing appropriate course content and programs.

The technical working group identified three primary content areas for fraud and forensic accounting curricula:

1. Criminology, specifically oriented to the nature, dynamics, and scope of fraud and financial crimes; the legal environment; and ethical issues
2. Fraud prevention, deterrence, detection, investigation, and remediation:[13]
   a. Asset misappropriation, corruption, and false representations
   b. Financial statement fraud
   c. Financial crime, fraud, and forensic accounting, in a digital environment, including:
      - Computer-based tools and techniques for detection and investigation
      - Electronic case management tools
      - Other issues specific to computerized environments
3. Forensic and litigation advisory services, including research and analysis, valuation of losses and damages, dispute investigation, and conflict resolution, including arbitration and mediation

The model curriculum, programs adopting the curriculum, and extensive details regarding the fields covered by the curriculum were examined in the November 2008 *Issues in Accounting Education*. This issue was devoted exclusively to fraud examination, forensic accounting, and financial forensics.

ROLE OF RESEARCH IN A PROFESSION

The long-term success of any professional endeavor is derived from three sources: research, practice, and education. Research drives professional innovation. Practitioners in the field implement the products of research (concepts, ideas, theories, and evidence) by applying, testing, and refining theory and research findings in the ‘‘real world.’’ Finally, educators create learning frameworks through which students benefit from the combined efforts of practice and research. For fraud examination, forensic accounting, and financial forensics to be a viable specialization over the long term, research opportunities and recognition are required to take the profession to the highest levels. To date, auditing and behavioral research focusing on fraud and forensic accounting issues has been published in many journals. In other related business disciplines, such as economics and finance, forensically grounded research has also been completed and published. Such efforts need to continue so that persons interested in both higher education and fraud and forensic practice have viable career opportunities.

Descriptive research, such as the ACFE’s biannual *Report to the Nation*, has been funded and completed by such organizations as the ACFE; AICPA; the large accounting firms; the U.S Department of Treasury; the Internal Revenue Service (IRS); the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Secret Service; the U.S. Postal Service; and others. Topics typically include:

- Is the incidence of fraud increasing or decreasing?
- What types of fraud are being committed?
- What is the cost of fraud?
- How is fraud committed?
- How is fraud detected?
- What are the victim profiles?
- What are the perpetrator profiles?

INSTITUTE FOR FRAUD PREVENTION

As documented by ACFE's 2008 *Report to the Nation*, despite the tremendous impact fraud and corruption have on our economy, there is relatively little research available on the costs of fraud, how it occurs, and why. Similarly, there exists no repository for gathering, storing, and disseminating fraud-related research findings and descriptive statistics. The primary goal of the Institute for Fraud Prevention (IFP) is to develop understanding of the causes and effects of fraud by serving as a catalyst for the exchange of ideas among top antifraud practitioners, government officials, and academics. The IFP is a voluntary association of organizations and researchers dedicated to fraud prevention, with an orientation toward research and education as a basis for developing antifraud best practices.

The IFP fulfills its mission in two ways:

1. Member organizations support research by selecting projects and providing funding, guidance, and data that will help better understand fraud with a long-term goal of reducing its incidence and effects.
2. The IFP's mission is to provide independent, nonpartisan expertise on antifraud policies, procedures, and best practices.

The IFP was founded by the ACFE and the AICPA. Current contributing members include Grant Thornton and D-Quest (a Japanese antifraud firm). A select group of intellectual partners, including the ATF, FBI, the U.S. Government Accountability Office, the U.S. Postal Inspectors, the National White-Collar Crime Center, and the Council of Better Business Bureaus, has provided guidance to the IFP.

The IFP identifies potentially fruitful research projects in the disciplines of accounting, law, psychology, sociology, criminology, intelligence, information systems, computer forensics, and the greater forensic science fields related to issues specific and unique to white-collar crime. In summer 2008, the IFP solicited white papers in several key areas in an attempt to identify the current body of knowledge. The five white paper topical areas and authors are:

1. "Financial Statement Fraud," by Joseph Carcello and Dana Hermanson
2. "The Legal Environment and White-Collar Crime/Forensic Accounting," by John Gill

3. ‘‘White-Collar Crime and Psychology, Sociology and Criminology,’’ by Sri Ramamoorti, Joe Koletar, and Daven Morrison
4. ‘‘Fraud and Forensic Accounting in a Digital Environment,’’ by Conan Albrecht
5. ‘‘Asset Misappropriation: Ethical and International Perspectives,’’ by Chad Albrecht, Mary-Jo Kranacher, and Steve Albrecht

Each white paper included a brief literature overview of past research (descriptive and investigative) at the beginning of the article and addressed these questions and issues:

- What do we currently know about the topical area?
- What research has been done?
- What are the lessons that we have learned?
- What don’t we know, and what are we missing?
- What additional resources are needed to do research on the topical area (additional theory, data, subjects, research methodology, etc.)?

Each white paper has underpinnings with practice, meaning that each one helps bridge the gaps between research findings and the implications to practitioners. It is believed that these research white papers will assist IFP members, intellectual partners, and academics understand the knowledge frontiers as they exist. The IFP Web site includes recent IFP studies and research, best practices, and antifraud resources for practicing professionals.[14]

ANTIFRAUD EDUCATIONAL PROGRAMS

Entities of all sizes are susceptible to both employee fraud (e.g., theft, embezzlement) and management fraud (e.g., manipulation of financial reports). Effective antifraud educational programs that focus on fraud awareness and education in the workplace environment, whistle-blowing policies and procedures of encouraging and protecting employees to report suspicious behavior, adequate internal control procedures designed to prevent and detect fraud, and conducting surprise audits can significantly reduce fraud. Antifraud educational programs should underscore antifraud functional responsibilities of all corporate governance participants described in this book and are summarized in Exhibit 14.2.

ANTIFRAUD APPLICATIONS FOR PRACTICE

John Adams: ‘‘The preservation of liberty depends upon the intellectual and moral character of the people.’’

Benjamin Franklin: ‘‘Only a virtuous people are capable of freedom.’’

Exhibit 14.2 Antifraud Functional Responsibilities

Audit Committee or Board of Directors	Senior Management	Internal Auditors	Independent Auditors	Certified Fraud Examiners
1. Supervise implementation of antifraud measures, including deterrence, prevention, and detection 2. Set a proper "tone at the top" 3. Actively evaluate management and provide an adequate feedback 4. Be keenly involved in the oversight responsibility over the financial reporting process 5. Consider the risk for the management override of controls and collusion 6. Relate the reported information to the forecasted or prior results 7. Consider feedback received from the independent auditors 8. Encourage transparency at all levels of controls 9. Include at least one financial expert	1. Be accountable for overseeing managers', supervisors', and employees' activities 2. Implement and monitor processes and controls 3. Adopt a proactive approach when dealing with fraud deterrence, prevention, and detection 4. Consider including a "management certification" statement in the annual reports (required for public companies) that addresses both financial reporting and internal controls	1. Develop and maintain sufficient knowledge to identify the indicators of fraud 2. Assess the fraud risk in the organization 3. Plan audits in accordance with industry standards and, where applicable, obtain audit committee (or the board of director) approval 4. Examine and assess the design and effectiveness of the system of internal control 5. Adopt a proactive approach in detecting corruption, misappropriation of assets, and financial statement fraud	1. Assist managers and audit committee (board of directors) by assessing the organization's process for identifying and responding to the risk of fraud 2. Ensure open and frank dialogue with the board, audit committee, and management regarding the entity's vulnerability to fraud	1. Assist managers and audit committee (board of directors) with deterrence, prevention, and detection processes (directly or with internal or independent auditors) 2. Provide input into managements assessment of fraud risk 3. Help to cultivate an appropriate anti-fraud environment 4. Assist the audit committee and board assesses susceptibility to management override and collusion 5. Resolve allegations or suspicions of fraud

Source: American Institute of Certified Public Accountants, "Management Antifraud Programs and Controls," 2002; available at www.aicpa.org/download/antifraud/SAS-99-Exhibit.pdf.

Thomas Jefferson: "In matters of style, swim with the current; in matters of principle, stand like a rock . . . The price of freedom is eternal vigilance."

George Washington: "There is but one straight course, and that is to seek truth and pursue it steadily. Our cruel and unrelenting enemy leaves us only the choice of brave resistance."

The United States is a nation of laws but, more important, America is a nation of people. Our globe is also a world made up of people—over 6 billion, and increasing daily. It is impossible that enough law enforcement exists to identify and prosecute every wrongdoing. Society exists, survives, and thrives not because of laws and enforcement but because of the choices people make. Laws, rules, and regulations cannot preserve a free and ethical society; people have that choice.

Most people choose to do the right thing. With regard to fraud, corruption, and abuse, the opportunity to commit some sort of wrongdoing exists, whether it is a smaller infraction such as violating travel policies to major defalcations such as financial reporting fraud that cost shareholders, creditors, stakeholders, and society billions. Insightful leaders of antifraud efforts, such as Joseph Wells and Steve Albrecht, have long recognized that fraud often is committed by good people making bad choices, choices that violate trust and end up hurting a lot of people, from faceless stakeholders to close friends and family.

Ethics is the heart of personal, economic, and social freedom. Facilitating good choices, difficult as they may be, is the responsibility of corporate governance professionals, including the board of directors, audit committee, senior managers, internal audit, external auditors, government, and regulators as well and managers, supervisors, line employees, and supporting staff. "A fish starts to stink at the head." Leaders lead by example, and organizations need to create environments where doing the right thing is as easy as possible.

While the words of our founding fathers provide great insight, some persons, no matter how supportive or strict the environment, will not do the right thing. Ethical choices and behavior are beyond their grasp. For that reason, we need the combined efforts of practice, research, and academia to develop and apply specialized skills to detect and investigate the types of nefarious activities presented in this book. Fraud examination, forensic accounting, and financial forensics are specializations at the heart of the antifraud fight. Their efforts, especially when combined with expertise from law, criminology, sociology, psychology, intelligence, computer forensics, and other forensic sciences, help level the playing field against the bad guys. Unfortunately, fraud examiners, forensic accountants, and financial forensics professionals are in a growth industry and will be quite busy for the foreseeable future. Nevertheless, forensics and antifraud professionals will keep fighting the good fight, making the right choices, and encouraging others to do the same.

The last thought:

Teachers open the door. You enter by yourself.

—Chinese proverb

NOTES

1. Dan Mangan, ‘‘Bailout ‘Big 4’ in Fraud Probe,’’ *New York Post*, September 28, 2008.
2. Kelli Arena, ‘‘FBI Probing Bailout Firms,’’ CNNMoney.com, September 24, 2008.
3. M. J. Epstein and A. D. Spalding, *The Accountant’s Guide to Legal Liability and Ethics* (Homewood, IL: Irwin Publishing Co., 1993).
4. Ibid., 190.
5. Z. Rezaee, A. Reinstein, and G. H. Lander, ‘‘Integrating Forensic Accounting into the Accounting Curriculum,’’ *Journal of Accounting Education* 2, No.1 (1996): 147–162.
6. National Commission on Fraudulent Financial Reporting, ‘‘Report of the National Commission on Fraudulent Financial Reporting’’ (October 1987), New York. A. Rezaee, G. H. Lander, and A. Reinstein, ‘‘Forensic Accounting: Challenges and Opportunities,’’ *Ohio CPA Journal* (August 1992): 20–25. Zabihollah Rezaee and E. James Burton, ‘‘Forensic Accounting Education: A Comparison of Academicians and Practitioners Opinions,’’ *Managerial Auditing Journal* 12, No. 3 (1997): 479–489.
7. AICPA, ‘‘Demand for Forensic CPA’s Accelerates, AICPA Survey Shows,’’ 2008; available at www.aicpa.org/download/news/2008/DEMAND_FOR_FORENSIC_CPAs_ACCELERATES.pdf.
8. Association of Certified Fraud Examiners, ‘‘About Us’’; available at www.cfenet.com/about/about.asp.
9. Public Oversight Board, *The Panel of Audit Effectiveness Report and Recommendations* (Stamford, CT: Public Oversight Board, August 2000).
10. Zabihollah Rezaee, A. Reinstein, and G.H. Lander, ‘‘Integrating Forensic Accounting into the Auditing Curriculum.’’ *Journal of Accounting Education* (Vol. 1, No. 2): 147–162.
11. Zabihollah Rezaee and E. James Burton, ‘‘Forensic Accounting Education,’’ available at www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=868372.
12. NIJ Web site, www.ncjrs.gov/pdffiles1/nij/grants/217589.pdf.
13. *Fraud prevention* refers to creating and maintaining environments where fraudulent activities are minimized. Fraud prevention contrasts with *fraud deterrence*, which refers to creating and maintaining environments where fraud is mitigated, subject to cost-benefit constraint.
14. Institute for Fraud Prevention, www.theifp.org.

Appendix

Summary of Six Recent Fraud Studies

Corruption or Compliance—Weighing the Costs: The 10th Global Fraud Survey (2007–2008) by Ernst & Young[1]

1. Corruption is still being seen by the businesses and executives as a prevalent problem. One-fourth of the organizations surveyed responded that they experienced corruption of some sort within the last two years.
2. Significant number of respondents felt that corruption is getting worse.
3. Number of cases prosecuted in OECD grows drastically from 51 cases in 2005 to 270 cases in 2007.
4. Businesses believe that laws and enforcements against bribery and corruption are getting stronger. Almost 70 percent of the respondents agreed to that statement.
5. Businesses are becoming more conscious in implementing anticorruption policies and procedures into their compliance practices Over two-thirds of the respondents suppose that their company's internal audit teams have adequate knowledge to uncover corrupt practices through compliance-focused audit.
6. Survey revealed that knowledge of FCPA and its requirements is insufficient. Fifty-eight percent of senior in-house counsel were not familiar with FCPA.
7. Survey disclosed that 44 percent of the companies did not have identifiable procedures in place to detect parties related to the government officials.

PricewaterhouseCoopers's 2007 Global Economic Crime Survey[2]

1. Survey discloses that fraud remains a considerable problem for the business, no matter what size of company it is. Over 43 percent of the respondents stated that they suffered some kind of economic crime in the last two years.
2. Respondents informed that after significant investment that companies made in fraud control, some form of fraud became less of a threat, but most of them did not change much.
3. Asset misappropriation became steadily less of a threat, while threats from money laundering, intellectual property infringement, and corruption and bribery have increased.
4. Survey indicated that all industries are more or less equally exposed to fraud. However, insurance sector has the highest total average cost to business ($5,494,831). It also reported the highest direct loss from fraud ($4,476,717) and spent, again on average, an additional $1,018,114 on managing the issues resulting from it.
5. Accounting fraud is prevalent in transportation and logistics (24 percent of the companies).
6. Study uncovered that the average loss from financial fraud increased significantly over the last two years (from approximately $1.7 million in 2005 to $2.4 million in 2007).

8. Most of the respondents agreed that setting up the successfully operating compliance program is a must in today's environment to prevent instances of bribery and corruption.	**7.** Asset misappropriation accounts for about 30 percent of average fraud losses, accounting fraud—12 percent.
	8. 41 percent of fraud was detected by chance; internal audit was able to detect fraud in 19 percent of the cases, while there was a large increase in the detection coming from whistle-blowing system, which indicates that companies are able to create an effective corporate culture.

KPMG Fraudster Survey 2007[3]	"How Executives View the Fraud Control Gap," Deloitte Forensic Center 2007[4]
1. Study demonstrates that fraud more likely will take place at the financial department, sales/operations, or the CEO level.	1. Companies perceive themselves as being less effective when it come to dealing with external fraud than internal fraud.
2. Ninety-one percent of the fraud executors performed multiple fraud transactions rather than a single transaction; every third executor performed more than 50 transactions.	2. Executives at the companies that perceive that their fraud control system is effective anticipated the instances of fraud will less likely occur in the next 12 months. Anticipations were divided as follows: 38 percent of the total answers anticipate misappropriation of assets to occur, 27 percent anticipate self-dealing fraud, and 24 percent anticipate improper expenditures.
3. Paramount motives were indicated as greed and opportunity (73 percent of the profiles).	3. The higher proportion of the senior executives is involved in fraud control system, the more effective the control is, but seemingly appears to be part but not all of what drives higher fraud control performance.
4. Forty-nine percent of respondents specified that internal control was too weak to prevent fraudulent actions.	4. Formal fraud control policies and strategies become are rapidly becoming a standard. Fifty percent of the respondents overall said that they a formal fraud control or policy.
5. Sixty-nine percent of the fraudulent actions were performed by the company's own employees, while the remaining 20 percent were performed by company's employees along with external perpetrators, and only 11 percent of the actions were performed by solely external individuals. So, employees represent the highest risk.	5. More effective companies address most fraud topics extensively in their fraud control policies or strategies.
6. The most effective methods for the fraud detection are whistle-blowing programs and management reviews.	6. Effective companies in 70 percent of the cases conduct formal fraud risk assessments, especially when it comes to the
7. In 50 percent of the cases, companies did not publicize the details of the fraud within the organization. Companies prefer	

to communicate information concerning fraud details selectively.

8. All sectors are equally affected by the white-collar crime, except for the chemicals, biotech, and pharmaceuticals sectors.
9. Every tenth fraudulent case was detected only after five years. That statistic emphasizes the need for actions in the area of fraud risk management.
10. Most of the respondents agreed that certain action should take place in order to mitigate fraud consequences and prevent fraud.

critical issues such as management override.

7. Whistle-blowers hotlines were adopted by 81 percent of the companies, but only 32 percent of the executives emphasized that their whistle-blowing hotline was effective.
8. Survey revealed an extensive opportunity for the improvement in the area of training employees about fraud control.
9. Executives recognize the role of technology in fraud monitoring and 28 percent confirmed that the intensification of the use of technology will likely occur in a next 12 months.
10. Forty-eight percent reported an increase in recourses devoted to the fraud due it increased publicity.

2008 Report to the Nation to the Occupational Fraud and Abuse (ACFE)[5]

1. Respondents indicate that they lose 7 percent of their annual revenue because of the fraud.
2. More than one-forth caused at least $1 million in losses.
3. Typical fraud usually lasted for at least two years before it was detected.
4. Financial statement fraud fell into the costliest categories, with a median loss of about $2 million among the 99 financial misstatements studied.
5. Forty-six percent of the fraud cases were detected by tips from affiliated parties. Consequently, tips are the most common method of fraud detection.
6. Study revealed that implementation of the fraud control systems leads to a reduction of the median losses from fraud.
7. Fraud affects many industries, but it is more likely to occur in financial services

2008 Corporate Fraud Task Force Report to the President[6]

1. According to the report, the Department of Justice has obtained nearly 1,300 corporate fraud convictions since 2002.

2. The FBI has undertaken several proactive Securities Fraud Market Manipulation initiatives that aggressively pursue corrupt participants in the financial markets.

3. The number of the investigations initiated increased significantly from 40 in 2006 to 124 in 2007.

4. Significant decline in incarceration rate can be observed in the last two years. The decline in FY2007 incarceration rate is the result of a larger number of sentenced cases identified as a corporate entity in the FY2007 data, when compared to FY2006. Corporate entities do not result in months to serve, and therefore reduce the incarceration rate.

5. According to the U.S. Postal Inspection Service Corporate Fraud Investigations

(15 percent), government (12 percent), and health care (8 percent).

8. Small businesses appear to be more vulnerable to fraud and usually have the higher losses.

9. Lack of the adequate internal control was cited as a most significant factor that allows fraud to proliferate by 35 percent of the respondents.

10. Most companies alter their antifraud controls after they discover they have been defrauded. The most typical change was to conduct management reviews of the internal controls (56 percent of the cases), then implementation of the surprise audit, then fraud training for employees and managers.

11. 29 percent of the fraud cases were committed by someone in the accounting department; 18 percent was committed by executives and upper management.

Statistics Fiscal Years 2004–2007 table, criminal fines obtained increased from $599,138 in 2006 to $19,185,000 in 2007.

6. Corporate fraud investigations involve the following activities: false accounting entries, bogus trades designed to inflate profits or hide losses, or false transactions designed to evade regulatory oversight.

7. Self-dealing insiders overlooked by the DoJ and FBI include the following practices: insider trading, kickbacks, backdating of the executive stock options, misuse of corporate properties for personal gain, and individual tax-violations related to self-dealing.

8. Fraud in connection with an otherwise legitimately operated mutual or hedge fund includes late trading, certain market timing schemes, falsification of net asset values, other fraudulent or abusive trading practices by, within, or involving a mutual or hedge fund.

Web links in order to the presentation in the table, from left to right:

1. info.worldbank.org/etools/antic/docs/Resources/Corruption_or_compliance_weighing_the_costs.pdf.
2. www.pwc.com/extweb/onlineforms.nsf/weblookup/GXENGCRIM2007Globaleconomiccrimesurvey:Download.
3. www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf.
4. www.deloitte.com/dtt/cda/doc/content/us_dfc_tenthingsfraudcontrol_200808%282%29.pdf.
5. www.acfe.com/documents/2008-rttn.pdf.
6. www.usdoj.gov/dag/cftf/corporate-fraud2008.pdf.

About the Authors

Dr. Zabihollah (Zabi) Rezaee and Dr. Richard (Dick) Riley are well-known accounting professors with substantial practice experience and expertise in anti-fraud practice and education, corporate governance and business ethics, and close working relationships with accounting firms and organizations. Collectively, the two authors have contributed substantially to the accounting profession and accounting education.

Dr. Rezaee is the Thompson-Hill Chair of Excellence and professor of Accountancy at the University of Memphis and served a two-year term on the Standing Advisory Group (SAG) of the Public Company Accounting Oversight Board (PCAOB). He received his B.S. from the Iranian Institute of Advanced Accounting, his M.B.A. from Tarleton State University in Texas, and his Ph.D. from the University of Mississippi. Professor Rezaee holds several certifications, including Certified Public Accountant (CPA), Certified Fraud Examiner (CFE), Certified Management Accountant (CMA), Certified Internal Auditor (CIA), and Certified Government Financial Manager (CGFM). Dr. Rezaee was also a finalist for the SOX Institute's SOX MVP 2007 Award. He has published more than 175 articles in a variety of accounting and business journals, served on the editorial boards of several journals, and made more than 180 presentations at national and international conferences.

In addition, Dr. Rezaee has published six books:

- *Financial Institutions, Valuations, Mergers, and Acquisitions: The Fair Value Approach*
- *Financial Statement Fraud: Prevention and Detection*
- *U.S. Master Auditing Guide*, third edition
- *Audit Committee Oversight Effectiveness Post-Sarbanes-Oxley Act*
- *Corporate Governance Post-Sarbanes-Oxley: Regulations, Requirements, and Integrated Processes*
- *Corporate Governance and Business Ethics*

Dr. Riley is currently a Louis F. Tanner Distinguished Professor of Public Accounting at West Virginia University and the 2008 Association of Certified Fraud Examiners' Educator of the Year. Since his appointment to the faculty of West Virginia University in 1998, his primary focus has been within the Business Masters Programs, encompassing Masters of Professional Accountancy, Graduate Certificate in Fraud and Forensic Accounting, Executive Master of Business Administration, and the Center for Executive Education and Development.

Dr. Riley is a forensic accountant and fraud examiner who has developed and implemented education programs for the United States National Institute of Justice and the Internal Revenue Service. In addition to his distinguished academic career, Dr. Riley was employed as a senior accountant in the accounting firm of Deloitte & Touche, and vice president, treasurer, and chief financial officer of Georgetown Leather Design Company, which had annual revenues in excess of $25 million dollars, and its ‘‘sister’’ company, Jordan Kitts Music, also had revenues approximating $25 million. Since 2002, Dr. Riley has performed expert financial analysis and litigation support for the mining, construction, and minerals processing industries and has extensive litigation experience beyond these businesses. He has also investigated the topical areas of biometrics for the biometrics industry and automated litigation support for the Department of Justice.

Dr. Riley possesses an undergraduate degree in accounting from Wheeling Jesuit University, a Masters of Professional Accountancy from West Virginia University, and a Ph.D. from the University of Tennessee. He serves on the Wheeling Jesuit Alumni Council as vice president and on West Virginia University's Academic Integrity Committee.

Index

Accountability, 4, 10, 16, 33, 44, 80, 113, 122
Accounting and Auditing Enforcement Releases, 118, 155, 270
Adelphia, 12, 28, 61, 122, 138, 184, 188–190
Advisory function, 131
American Institute of Certified Public Accountants, 5, 41, 91, 192, 230, 257, 311, 319
American Stock Exchange, 160, 174
Ames, Aldrich, 128
Antifraud program, policies, and education, 9, 19, 25, 48, 72, 89, 114, 135, 151, 178, 200, 225, 237, 254, 277, 302
Association of Certified Fraud Examiners (ACFE), 5, 29, 49, 50, 78, 243, 305, 311, 312, 321
Audit committee, 7, 8, 9, 10, 16, 17, 18, 20, 21, 22
Audit effectiveness, 17, 30, 215, 229, 243, 257, 271, 279, 315, 321
Audit failures, 14, 71, 273
Audit quality, 48, 230, 237, 262
Auditing standards, 5, 20, 33, 88, 118, 130, 164, 170, 175, 209
Auditor's independence, 38, 171, 222

Best practices, 4, 51, 53, 81, 82, 126, 131, 132, 143
Bill-and-hold sales, 65, 102
Blue Ribbon Committee (BRC), 166, 209, 227, 271
Board committees, 134, 138, 149, 150
Board of directors, 7, 8, 10, 12, 16, 17, 18, 22, 23, 24
Bristol-Myers Squibb, 97, 99–100, 116
British East India Company, 16
Business ethics, 233
Business roundtable, 142

Certified Fraud Examiner, 5, 29, 49, 50, 78, 243, 305, 311
Chen, David Jacob Levi, 105
Code of conduct, 49, 84, 106, 107, 193, 194, 217, 244
Committee of Sponsoring Organizations (COSO), 137, 188, 209, 239
Communication of fraud, 253
Compensation committee, 26, 148, 150, 151, 194
Continuous assurance and auditing, 298
Cooper, Cynthia, 51, 89, 112, 206, 211–212
Corporate culture, 19, 79, 81, 82, 97, 152, 197, 213
Corporate disclosures, 159
Corporate governance, 4, 8, 10, 14–25, 33, 41, 42, 48, 52, 66
Coughlin, Thomas M., 145

Digital economy, 283, 284–285
Discovery of fraud, 8

Earnings management, 17, 45, 80, 82, 97, 98, 103, 132, 172, 192
eBay, 285, 286, 287
Electronic commerce, 284, 285, 286, 287
Electronic financial reporting, 283, 285, 292, 293, 295, 297, 299, 301
Embezzlement, 5, 6, 19, 28, 61, 98, 214, 217, 318
Employee fraud, 5, 6, 19, 214, 235, 318

Enforcement procedures, 73, 264
Enterprise risk management, 107, 144, 197, 224
Enron, 3, 9, 11, 12, 13, 14, 18, 25, 27, 28, 30
Expert witnessing, 306, 308–310
Extensible business reporting language (XBRL), 40, 292
Extensible markup language (XML), 292–305
External audit function, 37, 67, 87, 130, 191
External auditors, 7, 8, 9, 10, 11, 17, 18, 23, 33, 38

Fair disclosure, 39, 266, 267, 295, 299, 300
Fair value accounting, 46
Fictitious assets, 101
Financial Accounting Standards Board, 32, 33, 257
Financial health, 34
Financial reporting system, 31, 32, 207, 272, 277, 285
Financial restatements, 9, 45–46, 52
Financial shenanigans, 88
Financial statement fraud, 4, 8, 32, 57, 78, 97, 122, 139, 159, 207, 229, 262, 288, 306
Foreign Corrupt Practices Act (FCPA), 195–196
Forensic accounting, 16, 29, 30, 72, 75, 153, 204, 278, 305–309, 311–318
Forensic accounting education, 315, 321
Forensic-type audit procedures, 17
Fraud, 3–30, 31, 34, 36, 38, 40–43, 45, 48–53
Fraud auditing, 245, 303
Fraud awareness education, 88–89
Fraud investigation, 76, 115, 204, 213, 310, 311, 312, 315
Fraud prevention program, 19, 73, 88–89, 236
Fraud risk factors, 96, 200, 202, 241, 245, 252, 253
Fraud schemes, 11, 65, 97, 100, 101, 102, 103, 114, 115, 116, 117
Fraud symptoms, 243, 247
Fraud vulnerability, 72, 310

Gamesmanship, 17, 23, 72–73, 112, 127, 194–196
Gamesmanship review, 72
Gatekeepers, 4, 10, 14, 67, 121, 123, 196, 236, 275
Generally Accepted Accounting Principles (GAAP), 24, 33, 83, 130, 167, 184, 231, 239, 261, 265, 272, 293, 299
Generally Accepted Auditing Standards, 130, 170
Global financial markets, 45, 309
Governing bodies, 18, 41, 42, 122, 123, 140, 158, 191, 207, 235

HealthSouth, 171–172
High-quality financial reports, 9, 39, 41, 184, 264
Hocus-pocus accounting, 103
HTML, 137, 257, 279, 292, 305

Independence rule, 170, 171, 183, 195
Independence Standards Board, 175
Independent audit, 4, 23, 24, 33, 34, 36, 37, 48, 68
Information technology, 94, 251, 284, 289, 302, 303
Institute of Internal Auditors (IIA), 50, 106, 131, 218, 314
Institute of Management Accountants (IMA), 314
Institutional investors, 44, 67, 69, 92, 126, 147, 149, 192, 264, 267
Intentional mistakes, 5
Interim financial statements, 17, 65
Internal audit services, 207, 221

Internal auditors, 9, 18, 23, 67, 72, 78, 81, 106, 107, 112, 118
Internal control, 8, 17, 19, 20, 21, 23, 26, 30, 32–34, 36–37, 40
International Accounting Standards Board, 43, 297
International Accounting Standards Committee (IASC), 293
International Financial Reporting Standards, 47–48, 272, 273, 297
Investor confidence, 4, 15, 31, 33, 37, 125, 142, 258, 259, 260
Irregularities, 4, 5, 9, 33, 68, 89, 109, 116, 124, 185, 189, 220, 230, 250

Key performance indicators, 43, 22, 193, 236
KPMG Survey, 198, 324

Legal counsel, 10, 67, 85, 87, 94, 108, 121, 131, 154, 158
Legal liability, 273, 321
Levitt, Arthur, 103, 118, 159, 183, 195, 205
Listing standards, 81, 126, 148, 150, 183, 198, 260
Litigation support consulting, 306, 308

Madoff, Bernard, 44, 271
Management fraud, 5, 6, 16, 19, 117, 118, 137, 183, 203, 204
Management motives and incentives, 191
Management responsibility, 147, 184
Market capitalization, 10, 11, 14, 45, 61, 63, 247, 284
Material weaknesses, 159, 168, 169, 185, 186, 188, 189, 223, 238, 240
Materiality, 40, 41, 95, 195, 215, 238, 244, 246, 247, 248
Materiality guidance, 246–249
Monitoring, 16, 58, 67, 68, 70, 71, 75, 76, 77, 81
Monitoring component, 220
Mutual funds, 9, 126, 285, 289, 290, 293

National Association of Securities Dealers, 17, 32, 41, 67, 158
National White Collar Crime Center, 317
New York Stock Exchange (NYSE), 17, 34, 67, 148, 158, 174, 198, 214
Nominating committee, director, 148, 150, 151

Oil-For-Food, 266
O'Malley Panel on Audit Effectiveness, 17, 243, 271
Omitted disclosures, 102
Organization for Economic Cooperation and Development, 133
Outside directors, 138, 145, 146, 149, 150, 157, 166, 271
Oversight function, 16, 37, 67, 71, 81, 127, 129, 133, 142

Phar-Mor, 3, 11–12, 28, 121–122, 124–125
Private Securities Litigation Reform Act of 1995, 111, 268–269
Professional skepticism, 17, 116, 234, 240, 243, 276
Privacy, 74, 283, 290, 291, 295, 300, 301, 302
Premature revenue recognition, 115, 201
Public Company Accounting Oversight Board (PCAOB), 33, 200, 209, 230, 231, 239, 260, 261, 273, 314
Public Oversight Board, 30, 279, 315, 321
Public trust, 4, 33, 229, 260

Quality financial audit, 17, 229
Qwest, 59, 76, 82–83

Reasonable assurance, 24, 111, 142, 177, 186, 199, 208, 218, 219, 229
Red flags, 86, 97, 105, 106, 109, 111, 114, 115, 116
Regulation FD, 267–268
Regulation S-K, 38
Regulatory bodies, 109, 245, 275
Related-party transactions, 80, 102, 103, 111, 207
Risk factors, 96, 106, 193, 200, 202, 241, 245, 249, 251, 252
Risk management, 10, 45, 107, 116, 130, 131, 134, 135, 136, 142
Rowley, Coleen, 51, 112

Sarbanes-Oxley Act of 2002, 3, 11, 57, 113, 121, 138, 161, 162, 164, 207, 230, 259, 260–263
SAS No. 70, 249
SAS No. 82, 2, 38, 216, 230, 233, 238, 241, 245, 250
SAS No. 84, 234
SAS No. 89, 188, 235
SAS No. 90, 235
SAS No. 99, 67, 106, 230, 234–235, 240, 242, 245, 251–253, 307–308
Satyam Computer Services LTD, 249, 272–273
Savings and Loan Crisis (1982), 3, 13
SEC's role in financial reporting, 265
Section 404 of SOX, 19, 32, 168, 186–187, 207, 215, 237
Security analysts, 45, 72, 195
Security, 10, 45, 51, 72, 97, 137, 195, 213, 255, 261
Sham transactions, 65, 101, 103, 104
Statement on Internal Auditing Standards (SIAS) No. 3, 209, 212, 213, 215
Stock-based compensation, 58, 68, 146, 192
Stock options backdating (2006), 3, 13, 26, 141

Transparency, 4, 10, 33, 39, 41, 80, 124, 125, 134, 170
Treadway Commission, 31, 32, 137, 177, 204, 209, 217, 227, 239, 312
Tyco, 262–263

Value reporting, 294
Verifiability, 40, 42
Vigilant audit committee, 85, 176
Voting system, 148, 149

Unqualified audit report, 24
U.S. capital market, 43, 126, 279
Users of financial statements, 23, 24, 39, 41, 45, 86, 185, 247, 270, 293

Waste Management, 3, 12, 28, 68, 70–72, 130, 233
Watkins, Sherron, 35, 51, 112
Webster, William, 159
Whistle-blowing, 8, 18, 19, 72, 81, 97, 112, 113, 118, 127
WorldCom, 3, 6, 9, 13, 14, 28, 29, 33, 51, 68

XBRL benefits, 293–294, 302
XBRL challenges, 293, 294–296
XBRL implementation, 301–302
XBRL taxonomies, 293
XML, 47, 155, 292, 300, 302

ZZZZBest, 3, 11, 27, 29, 57, 76

"*Financial Statement Fraud: Prevention and Detection, Second Edition* is a valuable reference guide for fraud examiners, audit committees, management, and regulators; and for one other important cog in this wheel: the investors who stand to lose everything."

—Joseph Wells, founder and Chairman, Association of Certified Fraud Examiners

Exceptionally well researched and fully revised, *Financial Statement Fraud, Second Edition* provides thorough coverage of the nature and extent of financial reporting fraud. Authors and accounting experts Zabihollah Rezaee and Richard Riley describe the most successful methods for preventing, detecting, and controlling incidents of financial reporting fraud and offer reliable guidance from standard-setting organizations such as the PCAOB, AICPA, and the SEC. Real-life case studies of companies guilty of such fraud—and a discussion of the consequences—help illustrate important concepts.

Thoroughly updated for today's marketplace, *Financial Statement Fraud, Second Edition* contains sample reports, examples, and documents that promote a realistic understanding of financial statement fraud and the investigation of fraudulent financial reporting allegations centered on the elements of fraud: the act, the concealment, and the conversion or benefit to the perpetrator.

Whether you are a manager, board of director, executive, or auditor, the *Second Edition* updates you on all the important issues regarding financial statement fraud, including:

- Auditing standards issued by the PCAOB, technological advances, and globalization
- SOX- and SEC-related implementation rules
- The movement toward IFRS and IAAS and the use of the XBRL reporting platform
- The trend toward reducing the complexity of the financial reporting process
- Corporate governance reforms in the post-SOX era
- Antifraud policies, practices, and education for all players in the financial reporting process

With practical tools and techniques for carrying out antifraud responsibilities, *Financial Statement Fraud, Second Edition* is the only resource you will need to identify early warning signs of financial misconduct and a reliable, practical guide to preventing it.

PREVENTION and DETECTION