CHAPTER 1

Introduction

ACCOUNTING AND AUDITING SCANDALS AND INTERNAL AUDIT

Despite all of the cataclysmic predictions of computer systems and other process-related disasters, the world survived the Y2K millennium change to the year 2000 with no major problems. However, the following year, 2001, became a real disaster for many U.S. accountants and auditors, as well as business in general. The long-running stock market boom, fueled by dot-com Internet businesses, was shutting down with many companies failing and growing ranks of unemployed professionals. Those same boom years spawned some businesses following new or very different models or approaches. One business that received considerable attention and investor interest at that time was Enron, an energy trading company. Starting as an oil and gas pipeline company, Enron developed a business model based on buying and selling excess capacity first over its competitors' pipelines and then moved to excess capacity trading in many other areas. For example, an electrical utility might have a power plant generating several millions of excess kilowatt-hours of power during a period. Enron would arrange to buy the rights to that power and then sell it to a different power company to get the latter out of a capacity crunch.

Enron applied its trading concept in many other areas, such as telephone message capacity, oil tankers, and water purification. Enron quickly became a very large corporation and got the attention of investors. Its business approach was aggressive but appeared to be profitable. Then, in late 2001, it was discovered that Enron was not telling investors the true story about its financial condition. It was found to be using off–balance sheet accounting to hide some major debt balances. It had been transferring significant financial transactions to the books of unaffiliated partnership organizations that did not have to be consolidated into its financial statements. Even worse, the off–balance sheet entities were paper-shuffling transactions

orchestrated by Enron's chief financial officer (CFO), who made massive personal profits from these transactions. Such personal transactions were prohibited by Enron's Code of Conduct, but the CFO requested the board to formally exempt him from code violations. Blessed by the external auditors, the board then approved these dicey off–balance sheet transactions. Once its behavior was publicly discovered, Enron was forced to roll these side transactions back in to its consolidated financial statements, making the numbers look very bad and forcing a restatement of earnings. Certain key lines of credit and other banking transactions were based on Enron's pledge to maintain specific financial health ratios. The restated earnings put Enron in violation of these agreements. What once looked like a strong, healthy corporation was not, and Enron was forced to declare bankruptcy in 2002.

Because Enron was a prominent company, many "How could this have happened?" questions were raised in the press and by government authorities. Another major question was "Where were the auditors?" Commentators felt that someone should have seen this catastrophe coming if they had only looked harder. The press at the time was filled with articles about Enron's fraudulent accounting, the poor governance practices of Enron's board, and the failure of its auditors. The firm of Arthur Andersen had served as Enron's external auditors and also had assumed its internal audit function through outsourcing. With rumors that the Securities and Exchange Commission (SEC) would soon be on the way to investigate the evolving mess, Andersen directed its offices responsible for the Enron audit to clean-up all related records. The result was a massive paper-shredding exercise, giving the appearance of pure evidence destruction.

The federal government moved quickly to indict Andersen for obstruction of justice, effectively ending its 90-year run as an auditor under a cloud of scandal. In June 2002, Andersen was convicted by a Texas jury of a felony, fined $500,000, and sentenced to five years' probation. With the conviction, Andersen lost any level of public and professional trust. In the end, this formerly "Big 5" public accounting firm has essentially ceased to exist. In early 2003, Andersen was operating primarily as a used furniture dealer, selling the furniture and fixtures from its closed offices.

At about the same time, the telecommunications firm WorldCom disclosed that it had inflated its reported profits by at least $9 billion during the previous three years. WorldCom soon declared bankruptcy, and the telecommunications company, Global Crossing, failed at about the same time when its shaky accounting became public. The cable television company Adelphia failed in 2002 when it was revealed that top management, the founding family, was using company funds as a personal piggy bank, and the chief executive officer (CEO) of the major conglomerate Tyco was both indicted in 2002 and fired because of major questionable financial transactions. Only a few examples are mentioned here; in late 2001 and early 2002,

many large corporations were accused of fraud, poor corporate governance policies, or sloppy accounting procedures. The press, the SEC, and members of Congress all declared that auditing and corporate governance practices needed to be fixed.

Public accountants and their professional organization, the American Institute of Certified Public Accountants (AICPA), received much of the initial criticism. The AICPA was responsible for financial auditing standards, and it governed public accounting quality standards through a peer review process. Because of Enron and the other failures, members of the U.S. Congress felt the existing process of establishing auditing standards and monitoring public accountants was not working. Although the AICPA initially resisted, the result was the Sarbanes-Oxley Act (SOA), passed in 2002. The most major and radical set of financial auditing changes in the United States since the 1930s, SOA has caused radical changes and strong new rules for public accounting, corporate governance, and others. Internal audit is one of those other groups. Although not specifically highlighted in the legislation, SOA has created some new rules and responsibilities for internal audit. In addition to SOA, a large number of other rules, improved standards, and technology developments are changing the environment for the internal audit professional.

WHAT ARE THE NEW RULES?

The Sarbanes-Oxley Act, with its public accounting firm regulatory authority, the Public Corporation Accounting Oversight Board (PCAOB), is a major component of new rules. SOA rules and other new standards and developments create a changed environment for the internal audit professional. A goal of this book is to introduce these new rules from the perspective of internal auditors and audit committee members with responsibility for their internal audit functions. We explain and interpret these processes and rules, giving some guidance on their effective implementation. The following paragraphs summarize this book on a chapter-by-chapter basis.

Chapter 2: Internal Audit and the Sarbanes-Oxley Act

An overview of the full SOA legislation is provided, with an emphasis on the requirements that will most impact internal audit, including relationships with external auditors and with the audit committee. The chapter also discusses the PCAOB (sometimes called "peek-a-boo" in the press) and its audit standards-setting responsibilities. With SOA, internal auditors will see major changes in their dealings with external auditors and the overall corporate governance processes. External audit firms are now barred from outsourcing the internal audit functions of their client companies and barred

from accepting audit client consulting assignments. In addition, the audit committee, or at least a designate, is required to take a much more active role in understanding internal control processes. While the PCAOB is too new and its start-up process has been moving slower than anticipated, that process is described, as well as progress to date.

Chapter 3: Heightened Responsibilities for Audit Committees

Corporate boards of directors have had audit committees for some time, although in the past some did little more than appoint external auditors and approve annual audit plans. The Enron audit committee, for example, met for less than one hour only once each quarter. SOA has created a heightened responsibility for the corporate audit committee. This chapter describes these SOA responsibilities and suggests how internal auditors might work more effectively with their audit committee. An audit committee's new responsibilities include establishing a code of conduct for corporate executives, launching a whistleblower function for the corporation, and supervising a formal assessment of internal controls. As part of its service to management role, internal audit should be in an ideal position to help its audit committee to achieve these responsibilities.

Chapter 4: Launching an Ethics and Whistleblower Program

Ethics or compliance programs have been common in larger corporations since the mid-1990s and have existed at some other organizations for much longer. The key element for any ethics program is a strong code of conduct. Such codes originally applied primarily to workforce-related issues, such as the company's sexual harassment policy, and they received only passing blessings from executives. SOA now mandates that such codes be established at a higher level and tailored for corporate executives. Whistleblower programs started with U.S. federal contract laws in the late 1980s and usually became part of corporate ethics programs. Many corporations today still have never initiated these programs or certainly have not carried them up to senior management. This chapter discusses how to establish both ethics and whistleblower programs, per SOA guidelines. It also suggests how internal audit can help to launch ethics and whistleblower functions where they do not exist and explains how to help make them SOA-compliant and how to perform reviews of these functions.

Chapter 5: COSO, Section 404, and Control Self-Assessments

Although some of the rules discussed in this book are completely new, the COSO (Committee of Sponsoring Organizations) internal controls review

framework has been with us since the mid-1990s and has been part of the AICPA's internal controls evaluation auditing standards. SOA reaffirms the importance of using the COSO approach to review and evaluate internal controls, and this chapter reintroduces COSO to internal auditors. The chapter provides an overview of the Organizational Sentencing Guidelines, a "carrot-and-stick" judicial approach to encourage effective compliance programs. Finally, the chapter discusses the Institute of Internal Auditor's Control Self-Assessment process, a methodology to review key business objectives, risks involved in achieving those objectives, and internal controls designed to manage those risks.

Chapter 6: Institute of Internal Auditors, CobiT, and Other Professional Internal Audit Standards

The Institute of Internal Auditors (IIA) recently has revised its Standards for the Professional Practice of Internal Auditing, the basic audit guidance for performing internal audits. All internal auditors should gain a basic understanding of these standards. This chapter provides an overview of these IIA Standards as well as the Information Systems Audit and Control Association (ISACA) CobIT control objectives framework. Not really a "standard," CobiT is a set of control objectives for understanding controls related to information systems. An uncomfortable acronym, CobiT stands for **C**ontrol **Ob**jectives for **I**nformation and related **T**echnology. Finally, IIA-oriented internal auditors involved in corporate-level audit activities often do not realize that a different professional group, the American Society for Quality (ASQ), has its own audit function and standards. ASQ internal auditors get involved in more quality assurance and process-oriented issues. The chapter introduces this group of auditing professionals and its standards.

Chapter 7: Disaster Recovery and Continuity Planning after 9/11

The World Trade Center terrorist acts of September 11, 2001, in New York became a major test for the effectiveness of information systems disaster recovery and continuity plans. Because of the extent of the destruction from this terrorist act, many established information systems disaster recovery plans did not work very effectively in the immediate aftermath. The result has been the introduction of new technologies and adjustments in emergency response approaches. What internal auditors once called disaster recovery now usually is called business continuity or business resumption planning, two separate but related concepts. This chapter introduces these topics as well as approaches for internal auditors to understand, review, and evaluate enterprise contingency planning in today's business environment.

Chapter 8: Internal Audit Fraud Detection and Prevention

Fraud can range from minor employee theft, to misappropriation of assets, to fraudulent financial reporting. The audit community, both external and internal, has perhaps for too long avoided procedures to prevent and detect financial fraud. Prior to SOA, for example, the AICPA mounted a major lobbying effort to declare that fraud detection was not its responsibility. As with so many things, SOA has changed these attitudes. This chapter provides guidance for internal auditors to help prevent and deter fraud at all levels. While there are few "new rules" here for fraud prevention and detection, auditor responsibilities are new. The chapter outlines how internal auditors can help to create a culture of honesty in their organizations, perform reviews to identify and mitigate fraud risks, and develop a fraud oversight process.

Chapter 9: Enterprise Risk Management, Privacy, and Other Legislative Initiatives

New rules for internal auditors have not just stopped with SOA and the IIA's new standards. This chapter discusses an important new ERM framework that has just been released in draft but soon will become important for management and auditors. We also introduce newer privacy-related rules and legislation that internal auditors should understand and consider in their reviews, when appropriate. Included here are the Healthcare and Insurance Portability and Accountability Act (HIPAA) and the Gramm–Leach–Bliley Financial Privacy Act (GLBA). Both of these outline some good practice minimum standards that internal auditors might consider in a variety of review areas.

Chapter 10: Rules and Procedures for Internal Auditors Worldwide

Although the IIA is an international organization, many of the new rules in this book focus primarily on current U.S. practices. SOA was passed by the U.S. Congress and is applicable only to companies whose securities are registered with the SEC. It is easy for non-U.S. auditors and professionals to say that this is just a U.S. problem and "We don't have those kinds of problems." There are movements in place to establish SOA-type procedures elsewhere in the world. This chapter reviews progress to date, with an emphasis on the United Kingdom's Turnbull Report and Canada's "CoCo" control objectives framework. The chapter also covers the importance of International Standards Organization (ISO) quality assurance guidance, the growing importance of the International Accounting Standards, and the SEC's efforts to extend SOA rules essentially worldwide. The chapter also discusses

the best practices Information Technology Infrastructure Library (ITIL) process standards for service deliver and service support.

Chapter 11: Continuous Assurance Auditing Future Directions

Processes that allow a continuous audit-type review of operations have been the realm of academic researchers and a few information systems auditors in recent years. The idea was to establish a set of auditing controls similar to what are installed in nuclear power plants. When processes go beyond some critical boundary, the warning lights go on and corrective actions are taken. This concept is beginning to receive more serious attention. The AICPA is currently in the midst of a task force to explore this area, and these concepts soon will become much more common. This chapter explores continuous assurance auditing concepts and ways internal audit can implement this change-the-rules auditing concept.

Chapter 12: Summary: Internal Auditing Going Forward

This chapter summarizes the most important of these new rules for today's internal auditors and speculates on future directions. SOA and the PCAOB are new entities that will evolve over time. However, the rules have changed or are changing for internal auditors going forward in the twenty-first century. While much of the focus here is on the larger public corporations, these rules will translate to smaller public, privately owned organizations as well as not-for-profit entities. We also can expect to see sustainability reporting audit requirements where auditors may review or assess environmental and social responsibility matters. All internal auditors should have an understanding of these new rules and how they will apply to circumstances in individual organizations.

WHO WILL FIND THIS BOOK USEFUL?

This book is directed to all internal auditors, with an emphasis on the chief audit executive (CAE). That key internal audit officer needs to understand SOA as well as the PCAOB and how they will apply to the organization. The guidance on establishing whistleblower functions, establishing an ethics practice, and establishing a good internal controls review and evaluation processes should help internal auditors to better communicate with designated members of the audit committees responsible for establishing these practices.

Under SOA, at least one member of a corporate audit committee must be identified as a "financial expert." This person should be someone with certified public accounting or CFO experience who understands generally

accepted accounting principles (GAAP) and accounting controls. The material in this book should help those designated financial experts to better understand the components of the COSO internal control model, to help initiate an effective whistleblower program in their organization, and to better appreciate the role of their internal audit function.

This book should be helpful to anyone interested in an overview of SOA and how it might apply to the organization. Although our interpretations of the act's text are just that, summaries and interpretations, the overview should provide the reader with a general overview of this important legislation. We also cover some technical areas, such as contingency planning today and setting up continuous auditing processes. These are described in such a way as to provide concepts to the technical auditor and a broad understanding to the audit manager and general reader.

Finally, this book should be of interest to anyone interested in good corporate and business governance. We are using "governance" here in broader terms than just the responsibilities of the board of directors in a public corporation. Since SOA's concepts will expand to a wide range of organizations, managers of public and private organizations of any size need to establish good governance practices. All should have in place ethical practices, effective internal controls, and some level of operations continuity planning.