CHAPTER 1

Introduction: Sarbanes-Oxley and Establishing Effective Internal Controls

As highlighted in the Preface, Sarbanes-Oxley (SOx) became U.S. law in 2002 and was the most sweeping set of new U.S. financial regulations since legislation passed in the 1930s aftermath of the Great Depression. SOx was enacted following a stream of major financial scandals at that time, with the accounting misdeeds at what was known as Enron Corporation[1] at the head of the pack, and lots of public concerns about poor corporate governance and public accounting practices. SOx created a new regulatory authority to set public accounting auditing standards, the Public Company Accounting Oversight Board (PCAOB), which essentially replaced the American Institute of Certified Public Accountants' (AICPA's) self-regulated auditing rule-setting authority, the Auditing Standards Board (ASB). Perhaps most important, SOx changed many of the processes that public companies had used for their own governance and to report their financial results to the Securities and Exchange Commission (SEC) in the United States and to the investing public. These SOx-initiated changes touched boards of directors, senior management practices, and the adequacy of the internal controls used to support financial and other processes.

SOx has had a major impact on the activities and responsibilities of auditors, whether external auditors, who now review the adequacy of reported standards following the PCAOB's auditing standards; internal auditors, who provide support and assurance to management and the audit committee on the adequacy of internal controls; or quality auditors, who assess the adequacy of other supporting processes. Each of these audit groups follows somewhat different standards and often has different objectives. Nevertheless, SOx has impacted all three audit groups. These are impacts that were developed by professional organizations and enterprises when

SOx was first launched and have evolved into various sets of best practices. The new PCAOB risk-based auditing standards, called *AS5*, however, have identified the need for all levels of auditors to change or at least reassess some of their SOx-related audit procedures.

The chapters that follow provide and discuss both definitions and suggested process improvements for these financial and operational internal controls, as well as supporting audit procedures. While many auditors are comfortable with these definitions, it may be sufficient here to say that internal controls are the types of procedures that consistently help assure that the "debits equal the credits" in accounting and business processes. Separation-of-duties rules are an example of a very simple internal control. One person might have the authority to initiate some financial transaction, but a separate person should be required to review and approve that same transaction. There is far less chance of fraud or even improper actions if two independent persons are involved in such a transaction. Although many enterprises have had good internal control rules and standards in place for many years, they often became much more informal between financial managers and the external auditors who reviewed and attested to them. Investigations into the failed Enron Corporation found many instances where its internal control processes, including overall corporate governance procedures, had very much failed.

The resultant corrective action here was the enactment of SOx. The U.S. Congress approved this legislation to correct what were viewed as a wide range of corporate governance and internal control shortcomings. The legislation was organized in a series of separate numbered sections covering specific areas of rules, which will be summarized in Chapter 2. As an example, SOx Section 404 rules require that management must first document and test their own internal controls, followed by an external auditor review and attestation of this enterprise internal control evaluation work. These SOx rules apply to any enterprise that has securities registered with the SEC. This could mean most major U.S. corporations, non-U.S. entities with stocks traded on U.S. exchanges, and many smaller enterprises.

Depending on an enterprise's size and annual report dates, SOx first became effective for larger corporations as early as late 2003. The rules have been relaxed and registration deadlines extended and further re-extended for foreign and smaller enterprises, but larger U.S. corporations today have been through at least two cycles of compliance with SOx rules. During its first years, SOx rules imposed major costs on many major U.S. corporations. As a result, many corporate managers and other observers saw little evidence of the value of these SOx-mandated internal control reviews. Perhaps it sounds a little too radical, but Scott McNealy, former CEO of Sun Microsystems, commented that the SOx procedures are like "throwing buckets of sand in

the gears of a market economy."[2] Similarly, a poll of IBM clients revealed that SOx compliance ranked as "the biggest ineffective and wasteful use of time for IT departments." There have been numerous other very unfavorable comments about SOx since it became law. A general industry and commentator consensus was that some changes to the SOx rules were necessary.

Changes Since SOx Was First Introduced

SOx is a large piece of legislation covering a wide range of corporate governance issues. For example, there are rules that a chief executive officer (CEO) cannot give out what were sometimes lavish "consulting" contracts to nonemployee members of the board, that investment analysts covering public companies must follow a code of conduct, and that external auditors cannot take over the responsibility for a client's internal auditors through outsourcing. Nonemployee director "consulting" fees were allegedly being used by some CEOs to buy off members of their board, and some analysts were telling outside investors to invest in a stock while they told their own investment bankers that the same stock was "junk." Similarly, the internal auditor outsourcing prohibition was designed to improve independence between internal and external auditors. Perhaps the most important sections of SOx for general and financial management, the board, internal audit, and other key members of the management team are:

- Section 404: Management Assessment of Internal Controls
- Section 302: Corporate Responsibility for Financial Report
- Section 409: Real Time Issuer Disclosures

An introduction and recommendations for an effective implementation of each of these sections and others will be provided in greater detail in later chapters. While many portions of SOx may require changes and adjustments, the Section 404 rules on internal controls have caused management and internal auditors the greatest level of pain and suffering. Strictly interpreted, the legislation laid out some very tight internal control compliance rules. Initially, the PCAOB mandated that the existing ASB-issued auditing standards should be used. The promise was that the PCAOB would soon issue its own internal control auditing standards.

As any auditor or financial manager involved in the first two years of the SOx Section 404 reviews knows, this process was really a scramble at many affected U.S. corporations. The former "Big Five" public accounting firms had been reduced to four with the fall of Arthur Andersen after the failure of Enron, and those remaining firms seemed to take extra steps to comply with every letter of the new and very detail-oriented PCAOB

issued SOx financial statement auditing rules, called *auditing standard number 2* (AS2). In addition, with Andersen gone, many corporations suddenly had a new external auditor.

An example of this complying-with-the-letter-of-the-law approach is the manner in which the issue of *materiality* was treated. Historically and before SOx, external auditors effectively ignored many smaller errors and omissions in their audits if they were not considered to be "material." Each of the major public accounting firms had their own measures here, but the idea was that if an error of misstatement was considered to be not material to the financial reporting results, the auditors would simply document the matter and move on. They considered errors that would not alter earnings per share by any more than some fraction of a cent not material. This concept is similar to speed limits on highways. If a road is posted for a speed limit of 65 miles per hour (mph), a driver faces little risk of being stopped for driving at 68 to 70 mph, under normal conditions. A driver speeding violation of 3 to 5 miles over the posted limit is just not considered to be material. Driving at more than 75 mph in a 65 mph zone may be another story.

Prior to SOx and its initial AS2 standards, these public accounting firm materiality measures seemed a little loose to outside observers. This author recalls one of his internal audit teams discovering an accounting error that involved tens of millions of dollars, only to have the external auditors tell the internal audit team that the error was not "material" for their purposes and to move on. The audit director—myself—and the audit team "bit their lips" on this matter. SOx rules have changed this. AS2 initially said that materiality should not be considered in reviews of internal controls. In effect, a $1 error was to be treated the same as a $1 million error—both were to be recorded as errors. Going back to our highway speeding example, this would say that a driver could be stopped and ticketed for speeding when driving 66 mph. Most drivers would view this as some level of lunacy.

While there were many other issues, the materiality consideration requirement was perhaps one of the issues raising the most complaints by corporate business executives in the United States. This attention to almost-trivial small problems took management's time and very much raised the costs of external audits. In its 2004 Audit Firm Performance Study, J.D. Power and Associates assessed SOx auditor performance through interviews with 1,007 audit committee chairs and 944 chief financial officers (CFOs). Nearly 90% of the CFOs involved in this study reported that the costs of compliance with SOx Section 404 requirements were greater than the resulting benefits. In addition, the study also showed that the accounting profession has experienced a decline in its performance ratings, with only 44% of the CFOs interviewed saying they had a high level of confidence in external auditors.[3]

These types of negative survey results, the throwing-sand-in-the-gearbox-type comments as mentioned above, and other negative comments encouraged some changed thinking in SOx rules by the PCAOB and the SEC. In addition, while SOx was originally enacted to cover all SEC registrants, including non-U.S. companies with securities traded through U.S. exchanges and very-low-capitalization smaller companies, many expressed concerns about the difficulty of establishing SOx compliance. To give non-U.S. and smaller corporations more time, the PCAOB extended the SOx compliance due dates for these two groups. Deadlines were extended and then extended again. At about the same time, the PCAOB announced in late 2006 that some of the more troublesome SOx compliance and enforcement rules would be changing.

The PCAOB has recently replaced its troublesome AS2 standard on auditing internal controls with an updated and more risk-based internal control auditing standard, AS5. Chapter 3 will introduce this new internal control auditing standard and will discuss how it impacts both internal and external auditors, as well as financial management. Some other PCAOB audit standards revisions are in process as this book goes to press, and the following section outlines some of these higher-level SOx changes. They will also be discussed more fully in Chapter 3.

PCAOB Internal Control Auditing Standards

As mentioned previously, auditing standards prior to SOx were developed and issued by the ASB, an appointed and very senior group of AICPA professionals. By auditing standards we are referring to the standards that external audit firms use to assess the accuracy and internal controls of the areas they are reviewing. They were published as numbered Statements of Auditing Standards (SASs). For example, SAS No. 99 describes the auditors' responsibility to identify fraud when performing reviews of financial statements. All AICPA external auditors are expected to follow this SAS No. 99 standard in any of their financial statement audits. For internal auditors, the Standards for the Professional Practice of Internal Auditing is a separate set of standards maintained by the Institute of Internal Auditors[4] (IIA) that applies to IIA members.

Developing and issuing SASs was a slow, ponderous process. Years ago, this author chaired a subcommittee of the ASB and was involved with developing and writing the then–SAS No. 55 on auditing IT general controls. It was not unusual to attend a subcommittee meeting to review an SAS draft where much discussion covered whether a section of the draft standard should say "the auditor *should*" or "the auditor *shall*." This is an important point, but such matters take lots of time.

After SOx became the law, the PCAOB stated that the existing SASs would be applicable until new replacements were issued. The PCAOB audit standards process here is different from the old days of the ASB. In the past, after the slow process of developing new SASs, the draft document was sent out for review and comment to a fairly wide group of auditing professionals. Their review comments would be used to modify the draft standard before developing the final SAS. This review process could take up to a year, followed by a long period prior to allow for actual implementation.

Although not that many standards have been issued to date, the PCAOB with SEC approval issues its auditing standards with a very limited time period for draft version review. For example, to initially aid external auditors in their reviews of internal controls, the PCAOB released its initial auditing standard on internal controls, called *AS2*,[5] quite quickly with limited time allowed for any draft version review and comment. That standard also was a good example of many of the common criticisms of governmental rules and regulations. AS2 contained over 150 pages of detailed requirements concerning the scope and reporting of an accounting firm's audit of a public company's internal controls over financial statements. This level of detail has often forced public accounting firms to audit internal controls too conservatively. Facing the risk of litigation for missing some small point, the public accounting firms under AS2 had a tendency to cover every point. Those original PCAOB-issued standards also gave no guidance to the enterprises on how to establish their internal controls.

AS2 caused a large amount of clamor and criticism, before the PCAOB announced its new internal control standard, AS5, in mid-2007. This more risk-based internal control auditing standard, described in Chapter 3, is a major change covering compliance with SOx Section 404 rules and should make the task less burdensome and onerous. In addition to Chapter 3 on AS5 and other PCAOB auditing standards, Chapter 9 talks about the importance of considering risks when establishing and evaluating internal controls, as well as the COSO Enterprise Risk Management (COSO ERM) framework.

Easing the Rules: Section 404 for Smaller Companies

When SOx was first launched, the SEC initially said it applied to any enterprise that had SEC-registered securities. While this seemed fair at first because a rule is a rule, this level of thinking meant that a relatively small, single business unit that has financed itself through a SEC-registered bond offering would be required to go through all of the same SOx procedures as a General Motors or a Microsoft Corporation. The PCAOB has given smaller enterprises more time to become compliant and has extended these due dates several times since. However, most reasonable persons would feel

that a regional chain of mortuaries, with a single small SEC-registered bond issue, should not have to go through the same SOx procedures as a General Motors.

Beyond just extending due dates, the PCAOB has made things a bit easier for the smaller enterprise. The new AS5 rationalizes SOx requirements somewhat and calls for consideration to be given to risks when assessing internal controls. In addition, the PCAOB has chastised the major public accounting firms for being almost too dogmatic in the internal control review work. The rules are easing a little, and we are beginning to see more rational and hopefully less costly approaches here going forward.

Foreign Registrant Rules

The initial set of SOx rules applied to any and all non-U.S. corporations that had securities registered with the SEC. There are numerous companies around the world that want access to U.S. capital markets through listings on one of the U.S. exchanges. However, these SOx rules initially implied that the SEC was proposing to regulate all non-U.S. markets as well. This raised an initial clamor on a whole series of levels and non-U.S. company rules have been somewhat softened. Also, similar to smaller domestic company rules, filing deadlines have been extended multiple times here.

Despite somewhat relaxed foreign registrant rules, some corporations are seeking to de-list and move to places like the London Stock Exchange, but this de-listing process is difficult. Even worse, many newer or expanding non-U.S. corporations are really thinking twice about going through the rigors of compliance with SOx rules.

CONVERGING TRENDS: ITIL, COBIT, AND OTHERS

When SOx became effective in the United States, it established a requirement for all SEC-registered enterprises to establish processes to better build, control, and monitor their internal controls. Almost concurrently with SOx, a raft of other U.S. regulations became law with often unpronounceable acronym names such as HIPAA, GLB, and FFIEC. In addition, with our increasing globalization of many areas of commerce, the International Organization for Standards (ISO)[6] has released standards with long numerical names such as ISO 9000:2000 as the international standard for defining the characteristics of quality management systems. The manager in a SOx environment trying to tie all these controls together needs often some better guidance to sort out these standards and to achieve more effective SOx compliance. Although managers and auditors in the very first years of SOx

Section 404 used a variety of home-bred, ad-hoc procedures to better manage their internal controls, three important frameworks go under the names of CobiT, ITIL and relevant ISO standards. This chapter will provide some highlights, and each are discussed in chapters following.

CobiT: Control Objectives for IT

CobiT is a control framework that was introduced many years ago by a professional organization then known as the EDP[7] Auditors Association (EDPAA), and has evolved and been enhanced over the years. Discussed in more detail in Chapter 5, the Control Objectives for IT (CobiT) is a worldwide-recognized framework or model for managing controls—particularly IT controls—in the enterprise. We have all but forgotten the meaning of the acronym *EDP*, and the EDPAA professional organization first evolved into the Information Systems Audit and Control Association (ISACA) and then to the very timely named IT Governance Institute.[8]

The more traditional, finance-background manager might back away from anything with IT in its name as something for the techies in the enterprise, but because IT processes are so essential and pervasive in the enterprise, the CobiT framework is an excellent tool for managing and understanding all levels of internal controls. CobiT supports SOx internal controls through setting a model and standards for IT governance with the concepts that an enterprise's IT resources should be aligned with the business, that they are resources that should be used responsibly, and that IT-related risks should be managed appropriately.

An earlier version of the CobiT framework was used by some enterprises during their first cycle of SOx 404 internal control assessments. The framework has since been upgraded and is now better linked to concepts such as Information Technology Infrastructure Library (ITIL) as well as to SOx. CobiT in its newest version 4.1 is a useful framework for documenting and understanding internal controls at all levels.

ITIL for IT Service Management

We have described CobiT as a framework that evolved from the IT audit profession—once called *computer auditors*—into an excellent framework for managing SOx corporate governance processes and overall IT governance. Discussed and introduced more fully in Chapter 8, ITIL is a set of published best practices that was first primarily used in essentially IT areas, but today is valuable for better managing SOx internal controls. ITIL got its start as a set of published books put together by the British government Central Computer and Telecommunications Agency, now the Office

of Government Commerce (OGC). ITIL evolved into a series of primarily IT-oriented best practices that first became widely used in the European Union (EU), and then gravitated to Australia, New Zealand, and finally Canada. Today, it is becoming widely recognized in the United States as well, with many enterprises embracing ITIL best practices. Names change over time, and many IT organizations are beginning to refer to this set of best practices as IT Service Management or ITIL Service Management. We will generally refer to this set of best practices as just ITIL.

In a somewhat different perspective than CobiT, ITIL is a tool to better align IT processes with overall business operations and is important for better understanding IT-related SOx internal controls in the enterprise. ITIL best practices are particularly valuable for matching or mapping IT operations and both CobiT and SOx internal accounting control points with what ITIL characterizes as customer relationship management. ITIL suggests that any non-IT business process has strategic, tactical, and operational elements. IT general and service-level management as well as change management processes should be in place to handle the supply-and-demand issues between these customer and IT organizations or entities. Exhibit 1.1 shows this relationship, and linkages at various levels. For example, service levels are defined and connected between business budget holders who contract for services and IT who manages this service level delivery. Chapter 8 will describe this relationship in greater detail.

ITIL represents an important set of best practices that will help an enterprise to better manage some and improve their internal controls. For example, IT and application system change management are important

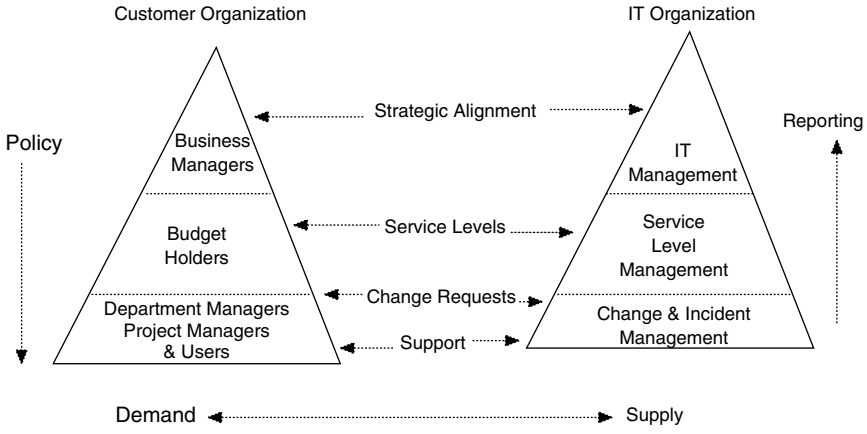

EXHIBIT 1.1 ITIL Customer Relationship Management

internal control processes for the entire enterprise. There should be a robust set of IT applications covering essentially all of its applications. However, internal controls break down if there are no strong processes in place to make certain that all such changes are properly authorized, tested, and otherwise approved before being placed into production.

ITIL best practices, as outlined in Chapter 8, provide some useful guidance for helping an enterprise to achieve SOx Section 404 compliance. In addition, this relationship with ITIL will help an enterprise to be compliant with both evolving IT best practices and SOx internal control requirements. ITIL provides an important set of tools to help improve the quality of an enterprise's IT operations.

ISO and Standards Convergence

As SOx takes on more and more of a worldwide focus and as all of our business operations become more global, the international standards known as ISO[9] are becoming important to U.S. enterprises. Although ISO standards have not historically directly impacted that many SOx activities, compliance with ISO standards is taking on an increasingly high level of importance, particularly as we become more of a global economy. Although these standards cover a wide variety of common processes and products (such as standards for the thread dimensions in an automobile bolt), the ISO standards covering quality management are important for maintaining effective internal controls.

ISO standards always have a number associated with them. For example, there is a series of ISO 9000 international standard standards for defining quality systems. Our goal is not to provide more than an overview of ISO standards, but Chapter 10 provides an description of several of the more important standards for internal controls improvement purposes. Enterprises worldwide use these standards, and their compliance is attested through a separate audit process.

Just as SOx or similar governance "SOx-like" guidance become rules on a worldwide basis, applicable ISO standards take an increasingly important role. Business professionals, and particularly internal and quality auditors, need to have an understanding of applicable standards such as ISO 9001 on effective quality management systems and how they map to SOx internal controls.

Whether it be SOx, CobiT, ITIL or others, a strong message throughout the following chapters of this book is that there is a growing convergence between these various governance standards and best practices. Internal audit standards are developed by their IIA professional organization, but quality management standards are issued by the Quality Audit Division

of the American Society for Quality.[10] Although these two internal audit disciplines have operated in very separate camps over the years, their practices are growing closer as time goes on.

We may soon see a growing level of convergence between the skills and practices of IIA-based internal auditors and those of quality auditors going forward. As discussed in Chapter 11, this an area of growing standards convergence. They will become important as all levels in the enterprise realize the growing significance of standards such as ITIL. There is always lots of new material to learn and master; subsequent chapters will attempt to introduce some of these very important areas.

ENDNOTES

1. For more information on Enron, a good read is Kurt Eichenwald, *A Conspiracy of Fools: A True Story*, Broadway, 2005.
2. *The Behind Business Line*, February 9, 2006, //www.thehindubusinessline.com/2006/02/09/stories/2006020900241100.1.
3. *Fraud* magazine, March/April 2005.
4. The Institute of Internal Auditors, Altamonte Springs, FL, www.theiia.org.
5. Auditing Standard No. 2: "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," www.pcaobus.org.
6. A French-language, Geneva, Switzerland–based organization; the correct acronym is ISO, www.iso.org.
7. EDP is an early-days computer system acronym that stands for *electronic data processing*.
8. IT Governance Institute, Rolling Meadows, IL, www.itgi.org.
9. The Geneva, Switzerland–based International Organization for Standards at www.iso.org, issues numbered ISO standards covering a wide variety of processes.
10. American Society for Quality, www.asq.org.