PART ONE

Auditing Internal Controls in an IT Environment

CHAPTER ONE

1 SOx and the COSO Internal Controls Framework

THE CONCEPT OF INTERNAL controls assessments has been around since the inception of auditing and has been an important concept going back to the early days of information technology (IT) auditing. Although there have been many definitions of internal controls, a good one for IT auditors is that internal control is a process, affected by an entity's board of directors, management, and other personnel, that is designed to provide reasonable assurance regarding the achievement of objectives in the categories of effectiveness and efficiency of operations, reliability of an enterprise's financial reporting, and an enterprise's systems and process compliance with laws and regulations. This well-recognized definition was established by the U.S. Committee of Sponsoring Organizations (COSO), an internal controls standards-setting authority that we will be discussing further in this chapter.

Audit professionals are responsible for reviewing and assessing enterprise management controls. Internal auditors do not construct and administer these controls—that is the responsibility of management. Auditors, acting as independent parties, both review and perform tests of enterprise internal controls to report to management and other parties whether they are adequate. These reviewers consist of both internal and external auditors, with external auditors in the United States following the rules and standards of the American Institute of Certified Public Accountants (AICPA). Internal auditors follow a similar but different set of standards and generally subscribe to the guidelines of the Institute of Internal Auditors (IIA), their international professional organization.

Both of these audit organizations have heritages going back to paper-and-pencil days, before today's pervasive use and reliance on IT systems and processes. Over the years, the Information Systems Audit and Control Association (ISACA) and its IT audit professionals have provided guidance for IT-related internal controls. IT auditors serve

in both external and internal audit roles, although most professionals may serve as internal auditors for their enterprises.

This chapter outlines the role of an IT auditor, particularly an IT internal auditor, in today's business enterprise. In addition, the chapter discusses two important IT audit concepts: the COSO internal control standards and the Sarbanes-Oxley Act (SOx) internal control review rules. Both COSO internal controls and SOx started as U.S. internal controls guidance rules but have become worldwide standards. They both had their origins as general financial and operations review standards and are now very applicable to IT audit environments as well.

Today's IT auditor must understand and use the COSO internal controls framework and SOx internal controls review procedures. Although these rules and procedures have origins in financial reporting and auditing, in today's IT-centric world, COSO internal controls and SOx are equally important to IT auditors. Enterprises need to follow these rules in order to assert or attest to regulators that their organizations have effective internal controls in place and that they are operating in compliance with those newer rules. The chapters in this volume rely on the internal control rules and procedures as we discuss a wide range of other IT audit, control, and security topics.

ROLES AND RESPONSIBILITIES OF IT AUDITORS

Much of this chapter and others focuses on the roles and responsibilities of an internal audit specialist, whom we call an IT or information systems auditor. Although sometimes serving as a member of a public accounting firm or outside consulting organization, IT auditors are generally members of an enterprise internal audit organization. An internal audit group is led by a manager with the title of chief audit executive (CAE) and is staffed by internal auditors with skills in reviewing and understanding operational and financial controls as well as compliance and regulatory issues impacting the enterprise. With IT processes and tools so pervasive in today's enterprise, all internal auditors should have a good understanding of IT controls and processes, but many internal audit functions require the skills of what we are calling an IT auditor.[1]

Traditional internal auditors always have had skills in understanding, testing, and evaluating what were once traditional paper-based controls and procedures. Starting in the 1970s, as enterprises started to build and implement more and more computer-based applications, they needed internal audit specialists who understood the new systems. Thus the role of the IT auditor was born.

The field once was called electronic data processing (EDP). Auditors are now sometimes known as information systems (IS) auditors or computer audit specialists; however, we are using the expression *IT auditor* throughout this book. An IT auditor is a specialist who follows the standards and principles of the IIA and often is a member of ISACA as well. There are many recognized specialist skills here, including the IT security procedures discussed in Chapter 19 and IT auditors skilled in computer-assisted audit tools and techniques (CAATTs), but most IT auditors are expected to have a strong

Auditor, Information Systems
JOB DESCRIPTION
Job Summary: Under direction of the Chief Audit Executive (CAE) and internal audit management, audits, reviews, tests, and evaluates IT-based applications and control procedures and reviews electronic security over the enterprise IT services network.

CHARACTERISTIC JOB TASKS AND RESPONSIBILITIES
May include any and/or all of the following:

1. Designs a technology-based audit approaches; analyzes and evaluates enterprise IT processes to assess internal controls and minimize risks; performs risk analysis of the enterprise's information technology infrastructure and services network; evaluates the possible risks of various computer systems; prepares reports documenting findings and risk assessment; evaluates management responses to findings and risk assessment.
2. Works independently or with other members of internal audit to review enterprise internal controls, following the COSO internal controls framework.
3. Examines the effectiveness of the information security policies and procedures; identifies inadequacies within the existing security program and possible action to be taken.
4. Develops and implements computer-assisted audit tools and techniques (CAATTs) to assist overall internal audit efforts and performs other IT-related tests of controls, as appropriate.
5. Develops and presents training workshops for audit staff on security controls and risk concepts.
6. Conducts and oversees investigation of inappropriate computer use.
7. Performs special projects and other duties as assigned; provides input on departmental administrative activities.

KNOWLEDGE, SKILLS, ABILITIES, AND PERSONAL CHARACTERISTICS

- Knowledge of auditing, information systems, and network security
- Investigation and process flow analysis skills
- Interpersonal/human relations skills
- Verbal and written communication skills
- Ability to exercise good judgment
- Ability to maintain confidentiality
- Ability to use IT desktop office tools, vulnerability analysis tools, and other IT tools

MINIMUM QUALIFICATIONS
Education and experience equivalent to:

- Bachelor's degree in computer science, computer programming, or accounting
- Certified Information Systems Auditor (CISA) credentials or candidate
- Certified Internal Auditor credential preferred

EXHIBIT 1.1 IT Auditor Job Description

general set of skills in evaluating IT-based internal controls. Exhibit 1.1 is a position description for a typical senior IT auditor.

This chapter emphasizes the importance of IT audit processes in performing internal controls reviews in today's heavily IT powered enterprises. IT audit specialists also have important key roles in the corporate governance of today's enterprise. They have skills that are unique but certainly should be adopted by all members of an internal audit team in expanding their IT knowledge and internal controls review procedures.

IMPORTANCE OF EFFECTIVE INTERNAL CONTROLS AND COSO

Internal control is one of the most important and fundamental concepts that external and internal auditors and business professionals at all levels must understand. The business professional builds and uses internal controls; auditors review and test the operational, IT, and financial systems and processes with a goal of evaluating their internal controls. Although internal and external auditors have different objectives, most of our references in this chapter apply to IT auditors, who have a major responsibility to understand and assess IT-related internal controls.

Although there have been many slightly different definitions of internal controls in the past, of COSO standards provides an appropriate definition. It recognizes that internal control extends beyond just accounting and financial matters and includes all enterprise processes. Also, because IT is so embedded into almost all business processes, IT-related internal controls are a major portion of our overall understandings of internal controls. An enterprise unit or process has good internal controls if it:

1. Accomplishes its stated mission in an ethical manner
2. Produces accurate and reliable data
3. Complies with applicable laws and enterprise policies
4. Provides for economical and efficient uses of its resources
5. Provides for appropriate safeguarding of assets

All members of an enterprise are responsible for the internal controls in their area of operation and for operating them effectively.

Despite or perhaps because of this broad and wide-reaching internal controls definition, many business professionals have had problems in fully understanding and applying internal control concepts. Looking at our definition a bit differently, the concept of an internal control and supporting control processes goes back to the basic mechanical and paperwork procedures that once existed throughout everyday life. Control processes are necessary for activities inside and outside today's enterprise, and many basic concepts and principles are the same no matter where the control is implemented. An automobile provides some basic controls examples. When the accelerator—a speed control—is pressed, the automobile goes faster. When the brake—another control—is depressed, the automobile slows or stops. When the steering wheel is turned, the vehicle turns. The driver *controls* the automobile, and all three of these represent the car's basic internal control system. If the driver does not use or improperly uses the accelerator, brake, or steering wheel, the automobile will operate *out of control*.

Expanding this concept just a bit, a stop sign, traffic direction sign, or gate crossing barriers all represent external controls to the auto and its driver. The driver is the operator of the automobile-based internal control process or system but has little decision authority over the message delivered from a traffic light external control.

From an internal control perspective, an enterprise can be compared to our automobile example. There are many enterprise systems and processes at work, such

as accounting operations, sales processes, and IT systems. If management does not operate or direct these processes properly, the enterprise may operate out of control. All members of an enterprise should develop an understanding of the appropriate control systems and then determine if they are properly connected to manage the enterprise. These systems are referred to as the enterprise's *internal control* systems.

Internal Controls Standards Background

Although the concept and definition of internal controls is fairly well understood today, this was not true until the late 1980s. The general concept may have been understood, but there was no consistent agreement among many interested about what was meant by ''good internal controls.'' Early definitions that first came from the AICPA and were used by the U.S. Securities and Exchange Commission (SEC) for the Securities Exchange Act of 1934 provide a good starting point. Although there have been changes over the years, the AICPA's first codified standards, called the Statement on Auditing Standards[2] (SAS No. 1) defined the practice of financial statement external auditing in the United States for many years. This AICPA definition of internal control has been subject to changes and reinterpretations over the years. Throughout the 1970s, the SEC and AICPA released many internal control definitions, and the major external auditing firms developed voluminous interpretations and guidelines.

Things changed in the late 1970s and early 1980s, a period when there were many major U.S. enterprise failures due to factors such as high inflation and the resultant high interest rates. Many times enterprises reported adequate earnings in their audited financial reports, only to suffer a financial collapse shortly after the release of favorable audited financial reports. A few of these failures were caused by fraudulent financial reporting, although many others were due to high inflation or other enterprise instability issues. Nevertheless, several members of Congress proposed legislation to ''correct'' these potential business and audit failures. Bills were drafted and congressional hearings held, but no legislation was passed.

In response to these concerns as well as the lack of legislative action, the National Commission on Fraudulent Financial Reporting was formed. It consisted of five professional organizations: the IIA and AICPA, mentioned previously; the Financial Executive International (FEI), an association of senior financial managers; the American Accounting Association (AAA); and the Institute of Management Accountants (IMA). The AAA is a professional organization for the academic accountants, and the IMA is the professional organization for managerial or cost accountants.

The National Commission on Fraudulent Financial Reporting came to be called the Treadway Commission after the name of its chairperson. Its major objectives were to identify causal factors that allowed fraudulent financial reporting and to make recommendations to reduce their incidence. The Treadway Commission's final report, issued in 1987, included recommendations to management, boards of directors, the public accounting profession, and others.[3] It also called for management reports on the effectiveness of their internal control systems and emphasized key elements in what it felt should be a system of internal control, including a strong control environment, codes of conduct, a competent and involved audit committee, and a strong internal audit function.

The Treadway Commission report again pointed out the lack of a consistent definition of internal control, suggesting further work was needed. The same Committee of Sponsoring Organizations that managed the Treadway report subsequently contracted with outside specialists and launched a project to define internal control. Although it issued no standards, the Treadway Commission released the COSO internal control framework, discussed in the next sections and referenced throughout this book.

COSO Internal Control Framework

As mentioned, COSO refers to the five professional auditing and accounting organizations that formed a committee to develop this internal control report; its official title is *Integrated Control–Integrated Framework*.[4] Throughout this book, we refer to it as the *COSO internal controls report* or *framework*. This is in contrast to COSO enterprise risk management (COSO ERM) enterprise resource management framework introduced in Chapter 4. First released in September 1992, the COSO internal controls report proposed a common framework for the definition of internal control as well as procedures to evaluate those controls. In a very short number of years, the COSO internal controls framework has become the recognized worldwide standard for understanding and establishing effective internal controls in virtually all business systems. The next paragraphs provide a fairly detailed description of the COSO internal controls framework and its use by internal auditors and business professionals for internal controls assessments and evaluations.

Virtually every public corporation has a complex control procedures structure. Following the format of a classic organization chart, there may be levels of senior and middle management in multiple operating units or within different activities. In addition, control procedures may be somewhat different at each of these levels and components. For example, one unit may operate in a regulated business environment where its control processes are very structured, while another unit may operate almost like an entrepreneurial start-up with a far less formal structure. Different levels of management in these enterprises will have different control concern perspectives. The question ''How do you describe your system of internal controls?'' might receive different answers from persons in different levels or units in each of these enterprise components.

COSO provides an excellent description of this multidimensional concept of internal controls, defining internal control in this way:

> Internal control is a *process*, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations[5]

Using this very general definition of internal control, COSO uses a three-dimensional framework to describe an internal control system in an enterprise. Exhibit 1.2

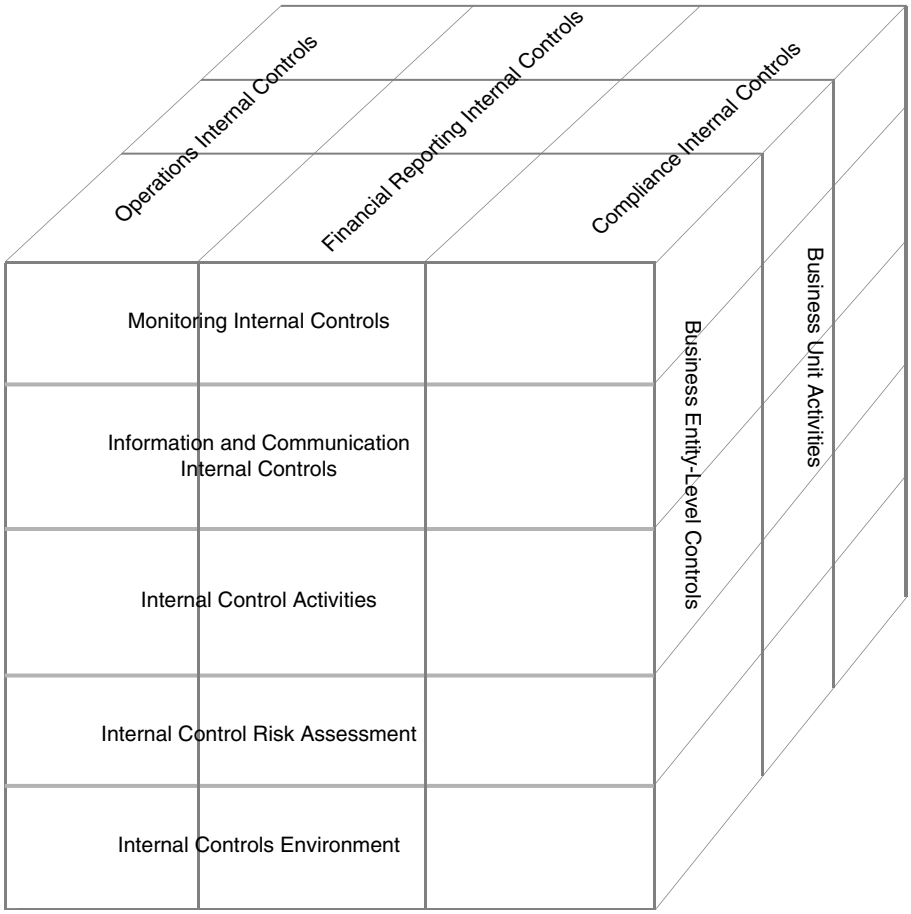

EXHIBIT 1.2 COSO Internal Controls Framework

describes this COSO internal control framework as a three-dimensional model with five levels on the front-facing side and the three major components of internal control—effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations—taking somewhat equal segments of the model with slices across its top. The right-hand side of the exhibit shows three segments, but there could be more, depending on the structure of the enterprise.

Each of the COSO internal control framework's levels, from Monitoring on top down to the Internal Controls Environment, is discussed in greater detail in the sections to come. The idea here is that when we look at the middle internal control activity layer—such as the period-end financial close—we should consider that control in terms of the business unit or entity or the multiple divisions on the side of the framework where that control has been installed. However, in this three-dimensional model, each control is related to all others in the same row, stack, or column.

The point of the COSO internal controls framework is that we should always consider each identified internal control in terms of how its components relate to

other associated internal control elements in the framework. In an example of end-of-period financial close internal controls, the enterprise should have information and communication links attached to the financial close processes, and the control should be monitored. Dropping down a level, there should be risk assessment activities associated with that financial controls process, and it should operate in an appropriate internal controls environment. Compliance and operations issues also contain factors for specific internal controls that may function at any level in the enterprise organization.

All IT auditors should have a strong understanding of the COSO internal controls framework. No matter what area is under review, IT auditors always need to review and consider internal controls in this type of a multilevel and three-dimensional manner. Starting with the first or bottom front-facing level, our text describes the COSO internal controls framework in greater detail.

Control Environment

The foundation of the COSO internal controls framework is what COSO calls the internal control environment, the foundation for all other components of internal control. It has an influence on each of the three objectives and all unit and entity activities. The control environment reflects the overall attitude of, awareness of, and actions by the board of directors, management, and others concerning the importance of internal controls in the enterprise. There are many fundamental concepts here, and each enterprise will have its own unique internal control foundation.

Enterprise history and culture often play a major role in forming this internal control environment. When an enterprise historically has had a strong management emphasis on producing error-free products and when senior management communicates the importance of high-quality products to all levels of the organization, the COSO control environment becomes a major enterprise internal control factor. The content and format of messages from the chief executive officer (CEO) or other senior managers are known as the tone at the top—management's messages to all stakeholders. However, if senior management has a reputation of looking the other way at policy violations, this same negative message will be communicated to other levels in the enterprise. A positive tone at the top by senior management is a key element of a strong enterprise control environment.

IT auditors should always try to understand and evaluate the overall control environment when performing virtually all reviews. When the internal control environment is weak, auditors almost certainly will find additional control concern areas. The control environment consists of the following components.

Integrity and Ethical Values. If the enterprise has developed a strong code of conduct that emphasizes integrity and ethical values, and if stakeholders appear to follow that code, all stakeholders will have assurances that the enterprise has a good set of values. A code of ethics or conduct is an important component of organizational governance. Internal audit codes of conduct are discussed in Chapter 3. However, even if an enterprise has a strong code of conduct, its principles can be violated through ignorance

rather than by deliberate employee malfeasance. In many instances, employees may not know that they are doing something wrong or may erroneously believe that their actions are in the enterprise's best interests. This ignorance often is caused by poor senior management moral guidance rather than by any individual employee intent to deceive. The enterprise's policies and values must be communicated to all organization levels. Although there can always be bad apples in any enterprise, strong moral messages will encourage everyone to act correctly. The objective should always be to transmit appropriate messages or signals throughout the enterprise.

All stakeholders, and certainly all internal auditors, should have a good understanding of their enterprise's code of conduct and how it is applied. If the existing code is out of date, if it does not appear to address important ethical issues facing an enterprise, or if management does not appear to be communicating the code to all stakeholders on a recurring basis, management needs to wake up and correct this deficiency. The code of conduct describes the rules for ethical behavior, and senior management should transmit a proper ethical message throughout the enterprise. Other incentives and temptations, however, can erode this overall control environment. Individuals may be tempted to engage in dishonest, illegal, or unethical acts if their enterprise gives them strong incentives or temptations to do so. For example, an enterprise may establish very high, unrealistic performance targets for sales or production quotas. If there are strong rewards for the achievement of these performance goals—or, worse, strong threats for missed targets—employees may be encouraged to engage in fraudulent or questionable practices to achieve those goals.

A strong internal audit function is a major component of the COSO control environment. If internal audit finds that management is placing constraints on the audit function, the CAE should remind senior management of internal audit's importance as part of the enterprise's overall internal control structure and, more important, should communicate these concerns to the board of director's audit committee.

Commitment to Competence. An enterprise's control environment can be seriously eroded if a significant number of positions are filled with persons lacking required job skills. An enterprise needs to specify the required competence levels for its various job tasks and to translate those requirements into necessary levels of knowledge and skill. By placing the proper people in appropriate jobs and giving adequate training when required, an enterprise is satisfying this important COSO control environment component.

Board of Directors and Audit Committee. The control environment is very much influenced by the actions of an enterprise's board of directors and its audit committee. An active and independent board is an essential component of the COSO control environment. By setting high-level policies and reviewing overall enterprise conduct, the board and its audit committee have the ultimate responsibility for setting this tone at the top.

Management's Philosophy and Operating Style. The philosophy and operating style of senior management has a considerable influence over an enterprise's control environment. Some top-level managers frequently take significant enterprise-level risks

in their new business or product ventures while others are very cautious or conservative. Some managers seem to operate by the seat of their pants while others insist that everything must be properly approved and documented. Some may take very aggressive approaches in their interpretations of tax and financial reporting rules while others go by the book. These comments do not necessarily mean that one approach is always good and the other bad.

These management philosophy and operational style considerations are all part of an enterprise's control environment. Although no one set of styles and philosophies is best for all enterprises, these factors such as a strong organization structure and effective human resource policies are important when considering the other components of internal control in an enterprise.

Organizational Structure. The organizational structure internal control component provides a framework for planning, executing, controlling, and monitoring activities to help achieve overall objectives. This control environment factor relates to how functions are managed and organized. Organizational structure is an important aspect of the enterprise's control environment, but no one structure provides any preferred internal controls environment.

An organizational structure is the manner or approach for individual work efforts to be both assigned and integrated for the achievement of overall goals. Every enterprise needs an effective plan of organization, and a weakness in organizational controls can have a pervasive effect throughout the total control environment. Despite clear lines of authority, however, enterprises sometimes have built-in inefficiencies that can become greater over time as they expand, causing control procedures to break down.

Assignment of Authority and Responsibility. The assignment of authority and responsibility in the control environment is similar to the organizational structure component just discussed. An enterprise's organizational structure defines the assignment and integration of the total work effort. The assignment of authority is essentially the way responsibilities are defined in terms of formal job descriptions and are structured in terms of enterprise organization charts. Although job assignments can never fully escape some overlapping or joint responsibilities, the more precisely these responsibilities can be stated, the better. The failure to clearly define authority and workplace responsibility often causes confusion and conflict between individual and group work efforts.

Human Resources Policies and Practices. Human resources (HR) practices cover personnel hiring, orientation, training, evaluating, and counseling, promoting, compensating, and taking appropriate remedial actions. Although the enterprise HR function should have adequate published policies and guidance materials, its actual practices should send strong messages to employees regarding expected levels of internal controls compliance, ethical behavior, and competence. The higher-level employee who openly abuses or ignores an HR policy quickly sends a message to other levels in the enterprise. The message grows even louder when a lower-level employee is disciplined for violating that same policy while everyone looks the other way at the higher-level violator.

Effective HR policies and procedures are a critical component in the overall control environment. Messages from the top of strong enterprise structures will accomplish little if the enterprise does not have strong HR policies and procedures in place. IT audit should always consider the HR element of the control environment when reviewing other parts of the internal control framework.

Summary. Just as a strong foundation is necessary for a multistory building, the control environment provides the foundation for the other components of internal control. An enterprise that is building a strong internal control structure should give special attention to placing solid foundation bricks in this control environment foundation. Of course, IT auditors should keep these concepts, such as effective HR policies, in mind when assessing internal controls. The COSO internal control environment does not require just a series of ''do the debits equal the credits?'' types of accounting rules but strong overall enterprise-wide policies that are effective.

Risk Assessment

The next level above the control foundation on the COSO internal control framework is risk assessment. An enterprise's ability to achieve its objectives can be at risk due to a variety of internal and external factors. Understanding and managing the risk environment are basic elements of the internal control foundation, and an enterprise should have a process in place to evaluate the potential risks that may impact attainment of its various objectives. This risk assessment component has its focus on internal controls within an enterprise and has a much narrower focus than the COSO ERM framework discussed in Chapter 4.

COSO internal controls risk assessment should be a forward-looking process that is performed at all levels and for virtually all activities within the enterprise. COSO describes risk assessment as a three-step process:

1. Estimate the significance of the risk.
2. Assess the likelihood or frequency of the risk occurring.
3. Consider how the risk should be managed, and assess what actions must be taken.

This COSO risk assessment process places the responsibility on management to assess whether a risk is significant and, if so, to take appropriate actions. COSO internal controls also emphasizes that risk analysis is not a theoretical process but often is critical to an entity's economic and operational success. As part of its assessment of internal control, management should take steps to assess the risks that may impact the overall enterprise as well as the risks over various enterprise activities or entities. A variety of risks, caused by either internal or external sources, may affect the enterprise.

The risk assessment element of the COSO internal controls Framework is an area where there has been much misunderstanding and confusion because of the similarly named COSO ERM framework discussed in Chapter 4. The risk assessment component of the COSO internal controls framework includes risk assessments for *within* an individual enterprise. The COSO ERM framework covers the entire entity and beyond. These are really two separate but related issues, and one is not a replacement for the other.

Control Activities

The next layer up in the COSO internal control framework is called control activities. These are the processes and procedures that help ensure that actions identified to address risks are carried out. Control activities exist at all levels and, in many cases, may overlap one another. They are essential elements to building and then establishing effective enterprise internal controls. The COSO internal controls framework identifies a series of these activities that are generally classified as manual, IT, or management controls; they are also described in terms of whether they are preventive, corrective, or detective control activities. Although no one set of internal control definitions is correct for all situations, COSO internal controls recommends these control activities for an enterprise:

- **Top-level reviews.** Management and internal auditors, at various levels, should review the results of their performance, contrasting those results with budgets, competitive statistics, and other benchmark measurements. Management actions to follow up on the results of these top-level reviews and to take corrective action represent a key control activity.
- **Direct functional or activity management.** Managers at various levels should review operational reports from their control systems and take corrective action as appropriate. Many management systems have exception reports covering these control activities. For example, an IT security system should have a mechanism to report unauthorized access attempts, with a control activity to follow up on reported events and take appropriate corrective action. Some of these activities link closely with the information technology infrastructure library (ITIL) best practices discussed in Chapter 7.
- **Information processing.** IT systems often contain controls to check for compliance in certain areas and then report any internal control exceptions. Those exception items should receive corrective action by automated systems procedures, by operational personnel, or by management. Other control activities include controls over the development of new systems or over access to data and program files.
- **Physical controls.** An enterprise should have appropriate control over its physical assets, including fixtures, inventories, and negotiable securities. An active program of periodic physical inventories represents a often significant control activity here, and IT auditors can play a major role in monitoring compliance here.
- **Performance indicators.** Management should relate sets of data, both operational and financial, to one another and take appropriate analytical, investigative, or corrective actions. This process represents an important enterprise control activity that can also satisfy financial and operational reporting requirements.
- **Segregation of duties.** Duties should be divided or segregated among different people to reduce the risk of error or inappropriate actions. This basic internal control procedure should be on almost every IT auditor's radar screen.

The control activities highlighted here represent only a small number of the many control activities performed in the normal course of business but involve policies

establishing what should be done and procedures to affect them. Even though control activities sometimes may be communicated only orally, they should be implemented thoughtfully, conscientiously, and consistently. This recognition and communication of control activities is a strong message for internal auditors reviewing such internal control activities. Even though an enterprise may have a published policy covering a given area, there should be established internal control procedures to support that policy. Procedures are of little use unless there is a sharp focus on the condition to which the policy is directed. All too often, an enterprise may establish an exception report as part of an automated system while that exception report receives little more than a cursory management review by its recipients. However, depending on the types of conditions reported, those exceptions should receive appropriate follow-up actions, which may vary depending on the size of the enterprise and the activity reported in the exception report.

These control activities should be closely related to one another to identify risks from the COSO internal controls risk assessment component. Internal control is a process, and appropriate control activities should be installed to address identified risks. Control activities should not be installed just because they seem to be the right thing to do, even if there are no significant risks in the area where the control activity would be installed. Sometimes control activities may be in place that perhaps once served some control risk concern, although the concerns have largely gone away. A control activity should not be discarded because there has been no recent history of control violations, but management needs to reevaluate these relative risks periodically. All internal control activities should contribute to the overall control structure, and IT auditors should keep this concept in mind as they review internal controls and make recommendations.

The COSO internal controls framework emphasizes that control procedures are needed over all significant IT systems: operational, financial, and compliance related. COSO internal controls breaks down information systems controls into the well-recognized general and application controls. General controls apply to much of the information systems function to help ensure adequate control procedures over all applications. A physical security lock on the door to the IT server center is such a general control for all applications running within that facility. IT general controls are discussed in Chapter 6. Application controls, discussed in Chapter 10, are also important IT control areas for evaluating the overall adequacy of internal controls. The COSO internal controls framework document concludes with a discussion of the need to consider the impact of evolving technologies; it should always be considered when evaluating IT control activities. Due to the rapid introduction of new technologies, what is new today will soon be replaced by something else.

Communications and Information

The COSO internal controls framework in Exhibit 1.2 describes most internal control components as layers, one on top of another, starting with the control environment as the foundation. As another way to look at the framework, Exhibit 1.3 describes the COSO framework as a pyramid-shaped model with the information and communication component as a side element that spans across other components. As important portions

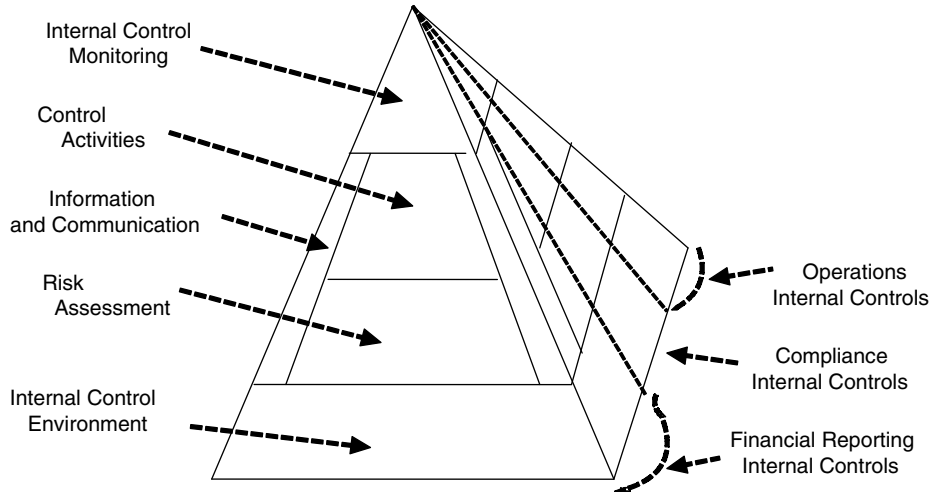

EXHIBIT 1.3 COSO Internal Controls Foundation Components

of the internal control framework, information and communications are related but distinct components. Appropriate information, supported by IT systems, must be communicated up and down the enterprise in a manner and time frame that allows people to carry out their responsibilities. In addition to formal and informal communication systems, enterprises must have effective procedures in place to communicate with internal and external parties. As part of any evaluation of internal controls, there is a need to understand these information and communication flows in the enterprise.

An enterprise needs information at all levels to achieve its operational, financial, and compliance objectives. For example, the enterprise needs information to prepare financial reports that are communicated to outside investors as well as internal cost and external market preference information to make correct marketing decisions. This information must flow both from the top levels of the enterprise on down to lower levels as well from lower levels back to upper levels. COSO internal control takes a broad approach to the concept of information systems, recognizing that they can be manual, automated, or even conceptual. Any of these information systems can be either formal or informal. Regular conversations with customers or suppliers can be highly important sources of information and are an informal type of an information system. The effective enterprise should have information systems in place to listen to customer requests and/or complaints and to forward that customer-initiated information to appropriate personnel.

COSO internal controls also emphasize the importance of keeping information and supporting systems consistent with overall enterprise needs. Information systems adapt to support changes on many levels. IT auditors, for example, often encounter cases where an IT application was implemented years earlier to support different needs. Although its controls may have been good, the system may not support the enterprise's current needs. COSO internal controls take a broad view of these types of systems and point to the need to understand both manual processes and automated technologies.

Monitoring

The pyramid view of COSO internal controls shows the monitoring component as the capstone, upper level of the COSO internal control components. Although internal control systems will work effectively with proper support from management, control procedures and both information and communication linkages must be in place to monitor all of these other activities. Monitoring has long been the role of IT auditors, who perform reviews to assess compliance with established procedures; however, COSO now takes a broader view of this control procedures monitoring. COSO internal control recognizes that control procedures and other systems change over time. What appeared to be effective when it was first installed may not be that effective in the future due to changing conditions, new procedures, or other factors.

A monitoring process should be in place to assess the effectiveness of established internal control components and to take corrective action when appropriate. This internal control component cannot be relegated just to the internal audit while management seems to remain oblivious to other potential control problems. An enterprise needs to establish a variety of monitoring activities to measure the effectiveness of their established internal controls as well as through separate evaluations of ongoing internal control activities to monitor performance and take corrective action when required.

Many routine business functions can be characterized as monitoring activities, and COSO internal control gives examples of this important component of internal control:

- **Operating management normal functions.** Normal management reviews over operations and financial reports are an important ongoing monitoring activity, but special attention should be given to reported exceptions and internal control deviations. Internal control is enhanced if reports are reviewed on a regular basis and corrective action initiated for any reported exceptions.
- **Communications from external parties.** External communication monitors, such as a customer complaint telephone number, are important, and the enterprise needs to monitor closely the messages from these calls and initiate corrective actions based on the calls when appropriate.
- **Enterprise structure and supervisory activities.** Senior management should always review summary reports and take corrective actions, but the first level of supervision often plays an even more significant role in monitoring. Direct supervision of clerical activities, for example, should routinely review and correct lower-level errors and assure improved clerical employee performance. This is also an area in which the importance of an adequate separation of duties is important, and dividing duties between employees allows them to serve as a monitoring check on one another.
- **Physical inventories and asset reconciliation.** Periodic physical inventories, whether of storeroom stock, negotiable securities, or IT assets, are an important monitoring activity. An annual inventory in a retail store, for example, may indicate a significant merchandise loss. A possible reason for this loss could be theft, pointing to the need for better security controls.

These are just a few examples of COSO internal controls monitoring activities. These types of procedures are often in place in many enterprises but are not thought of as ongoing monitoring activities. Any function or process that reviews enterprise activities on a regular basis and then suggests potential corrective actions can be thought of as a monitoring activity.

The COSO internal control framework points out the importance of ongoing monitoring activities and also suggests that ''it may be useful to take a fresh look from time to time'' at the effectiveness of internal controls through separate evaluations. The frequency and nature of these separate reviews greatly depend on the nature of the enterprise and the significance of the risks it must control. Management may want to initiate periodic evaluations of its entire internal controls, but most evaluations should be initiated to assess specific control areas. Often these reviews are initiated when there has been an acquisition, a change in business, or some other significant activity.

COSO also emphasizes that these evaluations may be performed by direct line management through self-assessment reviews. IT audit does not have to perform these reviews unless requested, and considerable time may pass before internal audit may schedule a self-assessment type of review in areas of operations. However, responsible management should consider scheduling and performing self-assessments on a regular basis. This type of internally generated review can point out potential control problems and cause operating management to take corrective action. Because these self-assessment reviews typically are not as comprehensive as normal internal audits, follow-up reviews should be launched if potentially significant problems are encountered through limited self-assessment reviews.

Internal Control Evaluation Process. The COSO internal controls guidance materials outline an evaluation process for reviewing internal controls. The evaluator should first develop an understanding of the system design, test key controls, and then develop conclusions based on the test results. This is really the IT audit process. COSO internal control also mentions *benchmarking* as an alternative approach. Benchmarking is the process of comparing an enterprise's processes and control procedures with those of peer enterprises. Comparisons are made with similar enterprises or against published industry statistics. This approach is convenient for some measures but filled with dangers for others. For example, it is fairly easy to benchmark the size, staffing levels, and average compensations of a sales function against comparable enterprises in the same general industry; however, the evaluator may encounter difficulties in trying to compare other factors due to the many small differences that make all enterprises unique.

Evaluation Action Plans. COSO internal control recognizes that many highly effective procedures are informal and undocumented. Many of these undocumented controls, however, can be tested and evaluated in the same manner as documented ones. An appropriate level of documentation makes any evaluation of internal control more efficient and facilitates employees' understanding of how the process works, but such documentation is not always essential. IT auditors reviewing an enterprise's internal financial controls systems always request to see systems documentation as part of their review work. If an existing process is informal, undocumented, but recognized as

effective, the review team will need to prepare its own action documentation to explain how the process works and the nature of its internal controls.

Reporting Internal Control Deficiencies. When internal control deficiencies are identified—whether through processes in the internal control system itself, monitoring activities, or other external events—they should be reported to appropriate levels of enterprise management. The key question for the IT audit evaluator is to determine what should be reported, given the many details that may be encountered, and to whom the reports should be directed. COSO internal control states that ''all internal control deficiencies that can affect the entity's attaining its objectives should be reported to those who can take necessary action.'' This COSO internal control statement makes sense but often is difficult to implement. The modern enterprise, no matter how well organized, is often guilty of a variety of internal control errors or omissions. COSO internal control suggests that all of these should be identified and reported and that even seemingly minor of errors should be investigated in order to understand if they were caused by overall control deficiencies. The COSO internal controls report uses the example of an employee's taking a few dollars from the petty cash fund. Although this could be viewed as a minor matter due to the small size of the theft, it still should be viewed as an overall control breakdown on several levels.

The monetary amount may not be significant, but COSO internal control urges that the matter be investigated rather than ignored, since ''such apparent condoning of the personal use of the entity's money might send an unintended message to employees.'' Prior to SOx, external auditors regularly applied the concept of materiality when performing reviews and decided that some errors and irregularities were so small that they were not material to the external auditor's overall conclusion. In the first years of SOx compliance reviews with the original Auditing Standard No. 2 (AS 2) guidelines, the message from many external auditors was that materiality issues should not be considered—an error is an error. This approach caused many managers to wonder why their external auditors were raising issues on what they felt were minor matters. With the AS 5 rules discussed later in the chapter, materiality and relative risk now must be considered when evaluating the efficiency and effectiveness of internal controls.

The COSO internal controls guidance concludes by discussing to whom to report internal control deficiencies in the enterprise. In one paragraph, COSO internal control provides guidance that is useful for evaluations:

> Findings on internal control deficiencies usually should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the enterprise whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.

The enterprise should also develop reporting procedures such that all internal control deficiencies encountered through IT audit reviews of ongoing operations are reported to appropriate levels of the enterprise. Management reporting and monitoring

is a highly important aspect of internal control. Internal audit has a lead role in that process through IT audit reviews and should be aware of the need for other monitoring processes when reviewing and evaluating internal controls.

Other Dimensions of the COSO Internal Controls Framework

We sometimes forget that the COSO internal controls framework should be reviewed and evaluated as the three-dimensional model, shown in Exhibit 1.2. In addition to the front-facing dimension of that model covering control activities, the right side covers entities or activities, and the top side or dimension of the framework cube covers the three dimensions of all internal controls:

1. Effectiveness and efficiency of operations
2. Compliance with applicable laws and regulations
3. Reliability of financial reporting

Each of the control areas just discussed—from the control environment to monitoring—should also be considered with respect to those other two dimensions.

Regarding the right side dimension, internal controls should be installed and evaluated across all units in the enterprise. This does not mean that a control activity, such as an expense approval process, must be identical in all units, such as at corporate headquarters or a sales office in a remote geographic location. However, there should be a consistent set of control processes throughout the enterprise with consideration given for the relative risks and scopes of operations. Internal controls should be consistent, but they should be applied appropriately in individual operating units.

The top dimension of the COSO internal controls framework is even more significant. It says that internal control activities should be installed in all enterprise operating units with respect to the three factors of internal controls: reliability of operations, regulatory compliance, and financial reporting effectiveness. Looking at internal controls from this three-dimensional viewpoint, there may always be some variations but the framework should be under a basic and consistent internal controls. Consider the example of a subsidiary facility in a central Asian nation, far away from its U.S. headquarters. Country expense approval procedures may be subject to local laws, and other processes may be somewhat different due to communication distances or differences in local IT systems. However, those internal controls still should be implemented in a manner that ensures reliability in financial reporting as results are reported to corporate headquarters.

All internal control considerations must be considered in terms of the COSO three-dimensional cube. That is, the control must be considered in terms of where it fits in the overall enterprise and its relationship to the three control objective areas just discussed. This concept provides IT auditors with a powerful way of looking at internal controls from a total perspective. The COSO internal controls framework continues to be an important standard and set of guidance materials for measuring and evaluating internal controls.

The COSO internal control framework is becoming the worldwide standard for building and developing effective internal controls. It is a continuous process in each of its three dimensions. On the front-facing side of the model, the monitoring component

on top is of little value unless internal control processes are in place all the way down to the internal control environment foundation. Similarly, effective internal controls must be installed in all levels of organizational units, and each of those controls must be sensitive to the three top-facing internal control elements.

COSO INTERNAL CONTROL SYSTEMS MONITORING GUIDANCE

Extensive guidance materials on the COSO internal controls framework have been available with sources ranging from AICPA auditing standards, various ISACA materials, and our own additional guidance materials.[6] However, many professionals had been seeking more specific guidance on how to implement COSO internal controls in business operations. A three-volume set of internal controls guidance materials was published by COSO in 2009.[7]

These volumes emphasize the importance of establishing processes to monitor the effectiveness and efficiency of established internal controls. Our previous description of the COSO internal controls framework, as shown in Exhibit 1.1, suggests that enterprises implement internal control monitoring processes in a manner similar to the way in which a manufacturing organization monitors the continued effectiveness and efficiency of its manufacturing procedures. The materials suggest that enterprises establish a four-phase or -stage monitoring process, as shown in Exhibit 1.4, where

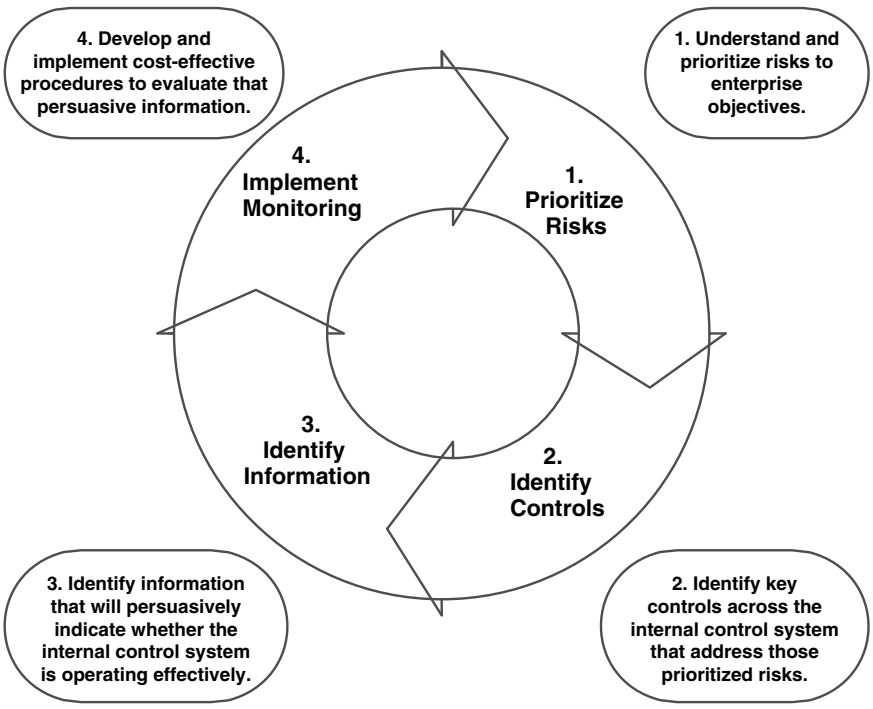

EXHIBIT 1.4 Monitoring Design and Implementation Process

an enterprise should first prioritize and understand the risks to its organizational objectives, then identify the controls that address those prioritized risks. IT auditors play a key role in the third step: identifying information that will persuasively indicate that the internal control system is operating effectively. The model calls for implementing cost-effective procedures to evaluate the information gathered through monitoring processes. The internal controls evaluation process is also very similar to the continuous assurance auditing procedures discussed in Chapter 14.

SARBANES-OXLEY ACT

The Sarbanes-Oxley Act (We will refer to the Act as SOx) is a U.S. law enacted in 2002 as a response to a series of accounting misdeeds and financial failures with an objective to improve public company financial reporting, audit, and enterprise governance processes. It first had a major impact on businesses in the United States and now is recognized worldwide. Although SOx's auditing and internal control rules have directly changed many external auditor practices, the act has also had a major impact on IT auditors. A general understanding of SOx, with an emphasis on its Section 404 internal accounting control rules, is a key knowledge requirement for all IT auditors.

Here we provide a high-level overview of SOx today with an emphasis on its Section 404, the rules that are most important to IT auditors. We summarize SOx requirements for reviews of internal accounting controls—a process important for IT auditors. In addition, we summarize the relatively new external auditing standards called Auditing Standard No. 5 (AS 5), a set of risk-based auditing approaches that also emphasize the importance of internal audit's work in performing financial reporting internal control reviews. IT auditors should have general knowledge and understanding of SOx internal control rules.[8]

Key Elements

The official name of SOx is the Public Accounting Reform and Investor Protection Act. It became law in August 2002 with most of the final detailed rules and regulations released by the end of 2003. Business professionals refer to it as the Sarbanes-Oxley Act, from the names of its principal congressional sponsors, which is shortened to SOx, SOX, or Sarbox, among many other variations.

SOx introduced a series of totally changed processes for external auditing and gave new governance responsibilities to senior executives and board members. SOx also established the Public Company Accounting Oversight Board (PCAOB), a rule-setting authority under the SEC that issues financial auditing standards and monitors external auditor governance. As happens with all financial and securities-related federal laws, an extensive set of specific regulations and administrative rules has been developed by the SEC based on the SOx legislation.

U.S. federal laws are organized and issued as separate sections of legislation called titles, with numbered sections and subsections under each. Much of the SOx legislation contains rules that are not that significant for most internal auditors and business

Title	Subject	Rule or Requirement
101	Establishment of PCAOB	Overall rules for the establishment of the PCAOB, including its membership requirements.
104	Accounting Firm Inspections	Schedule for PCAOB inspections of registered public accounting firms.
108	Auditing Standards	The PCAOB will accept current but will issue its own new auditing standards.
201	Out-of-Scope Practices	Outlines prohibited accounting firm practices, such as internal audit outsourcing, bookkeeping, and financial systems design.
203	Audit Partner Rotations	The audit partner and the reviewing partner must rotate off an assignment every five years.
301	Audit Committee Independence	All audit committee members must be independent directors.
302	Corporate Responsibility for Financial Reports	The CEO and CFO must personally certify their periodic financial reports.
305	Officer and Director Bars	If compensation is received as part of fraudulent/illegal accounting, the benefiting officers or director is required to personally reimburse funds received.
404	Internal Control Reports	Management is responsible for an annual assessment of internal controls.
407	Financial Expert	One audit committee director must be a designated financial expert.
408	Enhanced Review of Financial Disclosures	The SEC may schedule extended reviews of reported information based on certain specified factors.
409	Real-Time Disclosure	Financial reports must be distributed in a rapid and current manner.
1105	Officer or Director Prohibitions	The SEC may prohibit an officer or director from serving in another public company if guilty of a violation.

EXHIBIT 1.5 Sarbanes-Oxley Act Key Provisions Summary

professionals. For example, Section 602(d) of Title I states that the SEC ''shall establish'' minimum professional conduct standards or rules for SEC practicing attorneys. Although this rule perhaps is good to know, it does not have any IT audit impact. Exhibit 1.5 summarizes the major titles of SOx, although our focus is on Titles I and IV. Our intent is not to describe all of these sections or to reproduce the full text of this legislation—it can be found on the Web[9]—but to highlight portions of the law that are more significant to internal audit and business professionals. Of interest, even though internal control processes very much rely on both external and internal auditors, the original SOx legislation makes almost no direct references to the important roles and responsibilities of internal auditors. The importance of internal audit's role in SOx internal control reviews was highlighted subsequently in the AS 5 rules, released in mid-2007 and discussed later in this chapter. Our emphasis throughout is on the role of internal audit in today's SOx environment.

Title I: Public Company Accounting Oversight Board

SOx introduced significant new rules for external auditors. Prior to SOx, the AICPA had guidance-setting responsibility for all external auditors and their public accounting firms through its overall responsibility for the Certified Public Accountant (CPA) certification. Although state Boards of Accountancy actually license CPAs, the AICPA previously had overall responsibility for the profession. External audit standards were set by the AICPA's Auditing Standards Board (ASB). Although basic standards—called generally accepted auditing standards (GAAS)—have been in place over the years, newer auditing standards were released as numbered Statements of Auditing Standards (SASs). Much of GAAS was just good auditing practices—for example, accounting transactions must be backed by appropriate documentation—while the SASs covered specific areas requiring better definition. SAS No. 99, for example, covered the consideration of fraud in a financial statement audit. The AICPA's code of professional conduct required CPAs to follow and comply with all applicable auditing standards.

The AICPA's GAAS and its numbered SAS standards were accepted by the SEC, and these auditing rules defined external auditing standards and the tests necessary for an audited financial statement. However, the accounting scandals that led to the passage of SOx signaled that the AICPA-led process of establishing auditing standards was ''broken''; SOx took this audit standards-setting process away from the AICPA, which was dominated by major public accounting firms, and created the PCAOB, a nonfederal, nonprofit corporation with the responsibility to oversee all audits of corporations subject to the SEC.

The PCAOB does not replace the AICPA but assumes responsibility for the external auditing practices for AICPA members. The AICPA continues to administer the CPA examination, with its certificates awarded on a state-by-state basis, and sets auditing standards for U.S. private, non-SEC organizations. SOx Title I defines PCAOB auditing practices for external auditors; other audit process and corporate governance rules have changed how internal auditors coordinate their work with external auditors. Although SOx Title I contains many new rules, perhaps the three most important to IT auditors are that the PCAOB now has both major responsibility for public accounting firms, sets their external auditing standards, and sets audit standards rules such as workpaper retention. The next paragraphs briefly describe these SOx Title I external audit process rules.

- **PCAOB administration and public accounting firm registration.** The PCAOB is administered through an SEC-appointed board with required membership that is not dominated by CPA and public accounting firm interests. The PCAOB is responsible for overseeing and regulating all public accounting firms that practice before the SEC and for establishing auditing standards.
- **Auditing, quality control, and independence standards.** The PCAOB has the authority to establish auditing and related attestation standards, quality control standards, and ethics standards for registered public accounting firms. SOx recognizes previously issued AICPA auditing standards and has issued a limited number of new standards to date, such as AS 5 for the review and evaluation of internal controls. SOx rules further specify that an external auditor's evaluation must

contain a description of material weaknesses as well as any material noncompliance matters found. External auditors are required to update the effectiveness of internal controls, and an absence of this documentation should be considered a weakness of internal controls.

- **Audit workpapers retention.** PCAOB standard AS 3, *Audit Documentation*, mandates that audit workpapers and other supporting materials should be maintained for a period of not less than seven years. This requirement is in response to an infamous event just prior to the fall of the corporation that prompted SOx, Enron, and its auditor, Arthur Andersen. Enron was still in operation but was under some financial pressures when the SEC announced that it was going to conduct an onsite investigation. Enron's external auditors, Arthur Andersen, used an internal firm policy to justify destruction of all but the most current of their Enron audit documentation. This was a factor that led to the establishment of this SOx rule.
- **Scope of internal control testing.** PCAOB rules require external auditors to describe the scope of both their testing processes and their test findings. Prior to SOx, external auditors sometimes used internal firm policies to justify the smallest test sizes, and they frequently tested only a very small number of items despite being faced with very large test populations. If no problems were found, they expressed an opinion for the entire population based on the results of a very limited sample. External auditors now must pay greater attention to the scope and reasonableness of their testing procedures, and the supporting documentation must clearly describe the scope and extent of testing activities.

Title IV: Enhanced Financial Disclosures and Section 404

SOx Title IV is designed to correct some financial reporting disclosure problems, to tighten up conflict of interest rules for corporate officers and directors, to mandate a management assessment of internal controls, to require senior officer codes of conduct, and other matters. There is a lot of material here, but the most significant nugget for internal auditors is Section 404, Management's Assessment of Internal Controls. SOx requires that all annual 10K reports must contain an internal controls report stating management's responsibility for establishing and maintaining an adequate system of internal controls as well as management's assessment, as of the fiscal year ending date, of the effectiveness of those installed internal control procedures. These are what have popularly become known as the Section 404 rules. Internal and IT audit, outside consultants, and even the management team—but not the external auditors—have the responsibility to review and assess the effectiveness of their internal controls, and external auditors are then to attest to the sufficiency of the internal control reviews built and controlled by management.

Section 404 reviews are supported by the AS 5 standards discussed later in this section and are particularly important to internal auditors because the rules specify that external auditors may elect to use the work of internal auditors in their internal controls reviews. All IT auditors should have a basic understanding of SOx Section 404, whether they are acting as consultants in helping to build these internal accounting controls or acting in support of enterprise external auditors by auditing those internal accounting controls.

SOx Section 404 rules state that an enterprise is responsible for reviewing, documenting, and testing its own internal accounting controls, with those review results then passed on to the enterprise's external auditors, who are charged with reviewing and attesting to that work as part of their review of the reported financial statements. When SOx first became the law, Section 404 reviews were a major pain point for many enterprises because external auditors were required to follow a very detailed set of AS 2 financial accounting audit procedures that did not give any allowance for small errors or omissions. Section 404 auditing rules have changed with the release of AS 5 in 2007; a more risk-based audit approach also allows external auditors to better use the work of internal auditors in their assessments.

Section 404 Internal Controls Assessments

Management always has had the overall responsibility for designing and implementing internal controls over an enterprise's operations. Although the standards for what constituted good internal controls were not always that well defined in the past, they have remained a fundamental management concept. SOx Section 404 requires an annual internal control report, with these information elements, as part of an enterprise's SEC-mandated Form 10K annual report:

- A formal management statement acknowledging the enterprise's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- An assessment, as of the end of the most recent fiscal year, of the effectiveness of the enterprise's internal control structure and procedures for financial reporting

In addition, the external audit firm that issued the supporting audit report is required to review and report on management's assessment of its internal financial controls. Simply put, management is required to report on the quality of its internal controls, and its public accounting firm must audit or attest to that management developed an internal controls report in addition to the normal financial statement audit. Management has always been responsible for preparing periodic financial reports, and external auditors then audited those financial numbers and certified that they were fairly stated. With SOx Section 404, management is now responsible for documenting, testing and reporting on their internal financial controls effectiveness. External auditors then review the supporting materials leading up to that internal financial controls report to assert that the report is an accurate description of the internal control environment.

To the non–financial statement auditor and for some IT auditors, this might appear to be an obscure or almost trivial requirement. Even some IT auditors who perform operational audits primarily may wonder about the nuances in this process. However, this process follows a basic internal control on the importance of maintaining a separation of duties where the person who develops transactions should not be the person who approves them. Under Section 404 procedures, the enterprise builds and documents its own internal control processes, then an independent party such, as internal audit, reviews and tests those internal controls. Finally, the external auditors

review and attest to the adequacy of this process. Their financial audit procedures will be based on these internal controls. This Section 404 process improves things from pre-SOx days when external auditors frequently built, documented, and then audited their own internal controls—a separation-of-duties shortcoming.

Identifying Key Processes to Launch a Section 404 Compliance Review

Whether based on IT systems or even manual procedures, the basic processes for every enterprise should normally be considered in terms of some basic accounting cycles:

- **Revenue cycle.** Processes dealing with sales or other enterprise revenue.
- **Direct expenditures cycle.** Expenditures for material or direct production costs.
- **Indirect expenditures cycle.** Operating costs that cannot be tied directly to production activities but are necessary for overall business operations.
- **Payroll cycle.** Covers all personnel compensation.
- **Inventory cycle.** Although inventory eventually will be applied as direct production expenditures, time-based processes are needed for holding inventory until applied to production.
- **Fixed assets cycle.** Property and equipment require separate accounting processes, such as periodic depreciation accounting over time.
- **General controls IT cycle.** This set of processes covers IT controls that are general or applicable to all IT operations and are discussed in Chapter 6.

We will discuss some of these processes in Chapter 5 in the context of planning and performing effective IT audits. The identification of these key enterprise processes is an initial Section 404 compliance step, and an enterprise should document, understand, and test all of these ''key processes.'' IT audit often can be a major help here, as it may have already reviewed the prime systems and supporting IT processes through its annual audit reviews and documentation.

Internal Audit's Role

Even though SOx does not give specific responsibilities to internal audit, IT auditors are an important enterprise resource for the completion of Section 404 internal controls assessments. Under SOx, a separate and independent function within the enterprise—often internal or IT audit—reviews and documents the internal controls covering key processes, identifies key control points, and then tests those identified controls. External audit then reviews that work and attests to its adequacy. For many enterprises, IT audit can be a key resource for performing these internal controls reviews for technology-based processes. When SOx first became the law, internal audit functions often distanced themselves from Section 404 reviews because of potential internal auditor independence standards. The IIA Standards, as discussed in Chapter 3, now allow internal auditors to act as consultants to help document and establish effective internal control processes.

The CAE, financial management, and the audit committee should work with the enterprise's external auditors to define responsibilities for their Section 404 internal

1. Determine status of review: Is this the first round of Section 404 reviews for the entity or a subsequent-year follow-up?
2. If a new review, follow the work steps to understand, document, and test key processes. Otherwise, plan for a subsequent-period review.
3. Review the detailed documentation covering prior 404 reviews, including process flow charts, internal control gaps identified and remediated, as well as overall project planning documentation for prior review.
4. Review any recently published PCAOB rules covering Section 404 reviews and related auditing changes, and adjust review procedures to reflect those changes.
5. Meet with the external audit firm responsible for the current Section 404 attestations and determine if there are any changes in documentation and testing philosophy, with an emphasis on AS5 rules, from that prior review.
6. Consider any organization changes since the past review, including acquisitions or major reorganizations, and modify review coverage, if necessary.
7. Through meetings with senior and IT management, identify if new systems or processes have been installed over the past period and if those new changes have been reflected in updated documentation.
8. Review any internal control weaknesses identified in the past review, and assess whether internal control corrections reported as installed appear to be working.
9. Assess the status of existing Section 404 documentation, and determine the extent of new documentation preparation necessary.
10. Assuming the prior Section 404 review was done by internal audit, determine that appropriate knowledgeable, trained resources are available to perform the upcoming review.
11. Interview all parties involved in the prior Section 404 review exercise to assess any lessons learned and develop plans for corrective actions in the upcoming review.
12. Based on discussions with external auditors and senior management, determine scope materiality parameters for the upcoming review.
13. Determine that the software, if any, used to document prior review is still current, and make any changes necessary to have adequate tools in place to perform the upcoming review.
14. Prepare a detailed project plan for the upcoming Section 404 review, with consideration given to coordination of review activities at business entity units and external auditors.
15. Submit plan for approval by senior management.

EXHIBIT 1.6 Planning Considerations for a Section 404 Internal Controls Review

control reviews. These reviews are performed on an annual process, with documentation prepared and tested in the first year updated and retested in future periods. All parties should develop a cost-effective approach to achieve these SOx requirements and assess their IT applications and controls.

IT audit–led SOx Section 404 reviews should be planned and conducted like any new IT audit project as discussed in Chapter 5 on planning and developing effective IT audits. Exhibit 1.6 outlines some planning considerations for an IT audit–led Section 404 internal controls review. Internal audit can play a major role in helping senior management establish Section 404 compliance. Based on the internal audit standards discussed in Chapter 3, internal audit should recommend internal control improvements as the new processes are being developed, or internal audit can act as consultants for installing those new internal control processes.

AS 5 Rules and Internal Audit

Shortly after SOx became law in the United States, the PCAOB released its AS 2 guidance, which called for external auditors to take very conservative and detailed approaches on their audits of financial statements. AS 2 mandated a ''look at everything'' detailed audit approach, and enterprise external audit bills became much more expensive in those first SOx years. However, there were frequent complaints by industry leaders and others with a general consensus that AS 2 needed some revisions. The SEC and the PCAOB agreed to revise AS 2, and AS 5 was issued in late May 2007.

AS 5 is a set of standards for external auditors who review and certify published financial statements. The new rules are also important for internal auditors. AS 5 introduces risk-based rules with an emphasis on the effectiveness of internal controls, oriented to enterprise facts and circumstances. In addition, AS 5 calls for external auditors to consider including reviews of appropriate internal audit reports in their financial statement audit reviews. It allows external auditors to place more emphasis on management's ability to establish and document key internal controls.

AS 5 rules are particularly important for IT auditors because external auditors can rely on the work of internal auditors in their Section 404 assessments. AS 5 has three broad objectives:

1. **Focus internal control audits on the most important matters.** AS 5 calls on external auditors to focus their reviews on areas that present the greatest risk that an internal control will fail to prevent or detect a material misstatement in financial statements. This approach calls for external auditors to focus on identifying material weaknesses in internal control in their audits, before material misstatements of financial statements arise. AS 5 also emphasizes the importance of auditing higher-risk areas, such as the financial statement period-end close process and controls designed to prevent fraud by management. At the same time, the new standard provides external auditors a range of alternatives for addressing lower-risk areas, such as by more clearly demonstrating how to calibrate the nature, timing, and extent of testing based on risk, as well as how to incorporate knowledge accumulated in previous years' audits into the auditors' assessment of risk. Also very important to internal auditors, AS 5 allows external auditors to use the work performed by an enterprise's internal auditors, when appropriate.
2. **Eliminate audit procedures that are unnecessary to achieve their intended benefits.** AS 5 does not include the previous AS 2 standard's detailed requirements to evaluate management's own evaluation process and clarifies that an internal control audit does not require an opinion on the adequacy of management's processes. For example, AS 5 focuses on the multilocation dimensions of risk in an enterprise and reduces requirements that external auditors should test a ''large portion'' of an enterprise's operations or financial positions. This should allow a reduction in financial audit work.
3. **Make the financial audit clearly scalable to fit the size and the complexity of any enterprise.** In order to provide guidance for audits of smaller, less complex companies, AS 5 calls for tailoring internal control audits to fit the size and

complexity of the enterprise being audited. The standard has guidance on how to apply AS 5 to smaller, less complex enterprises as well as the units of larger enterprises.

Following AS 5, external auditors may consider using the work of others to help perform their SOx financial statement internal control audits. Although it was not as well defined under previous AS 2 rules, AS 5 now explicitly states that an external auditor may use the work performed by, or receive direct assistance from, internal auditors, other company personnel, or third parties working under the direction of management or the audit committee, to provide evidence about the effectiveness of financial reporting internal controls. This is a major change for internal auditors.

Of course, external auditors are signing off on or attesting to the audit results, and they must assess the competence and objectivity of the persons whose work they plan to use. The higher the degree of competence and objectivity of others, the greater use an auditor may use their work. In particular, AS 5 calls for an assessment of the competence and objectivity of internal auditors. *Competence* means the attainment and maintenance of a level of understanding and knowledge that enables persons to perform the tasks assigned to them, and *objectivity* means the ability to perform those tasks impartially and with intellectual honesty. To assess competence, an external auditor should evaluate the qualifications and ability of the internal auditors or others to perform the work the external auditor plans to use. To assess objectivity, AS5 calls for an external auditor evaluation of whether factors are present that either inhibit or promote a person's ability to perform with the necessary degree of objectivity the work the auditor plans to use.

AS 5 goes on to state that external auditors should not use the work of persons who have ''a low degree of objectivity, regardless of their level of competence,'' and also should not use the work of persons who have a low level of competence regardless of their degree of objectivity. Personnel whose core function is to serve as a testing or compliance authority at an enterprise, such as internal and IT auditors, normally are expected to have greater competence and objectivity in performing the type of work that will be useful to the external auditor. This may be an area where the CAE, as well as the audit committee and senior management, may want to challenge external auditors if they see no role for internal audit in this financial statement audit planning process.

Although AS 5 talks about internal auditors in an almost generic fashion, the role of the professional IIA member IT auditor is important here. Based on the IIA's International Professional Practice of Internal Auditing standards, as summarized in Chapter 3, an IT auditor can be expected to have the competence and objectivity necessary for help in supporting an external auditor's review of Section 404 internal controls. Although other persons, such as outside consultants, can be used to assist external auditors in their financial statement internal control reviews, IT auditors should have a major role here in assisting with Section 404 and AS 5 audit compliance.

Internal audit's ongoing role here should be viewed with a level of caution. We have discussed how IT auditors often are excellent resources to identify, document, and test key Section 404 internal control processes. They could do this in a support role for the external auditor's attestation reviews. However, pure separation-of-duties independence rules say

that they cannot perform these reviews, as internal auditors, within the enterprise and then act as a third-party helpmate for the external auditors to help attest to that same work. This conflict of duties should be clearly understood by all parties, and internal auditors and management should exercise care to prevent it.

WRAPPING IT UP: COSO INTERNAL CONTROLS AND SOx

This chapter has introduced two important concepts for IT auditors: the COSO internal controls framework and SOx internal controls standards. IT auditors work in a variety of enterprise environments, but today they will almost always encounter COSO internal control framework rules and SOx internal control review requirements under AS 5. Although this chapter provides just a summary description of each of these standards, and many auditors will require a greater understanding, all IT auditors should have a general knowledge and understanding of the COSO internal controls framework and SOx rules for understanding internal controls. These are worldwide standards requirements for today's effective IT auditor.

NOTES

1. More information on the total roles and responsibilities of internal audit in today's enterprise can be found in Robert Moeller, *Brink's Modern Internal Auditing*, 7th ed. (Hoboken, NJ: John Wiley & Sons, 2009).
2. Statement on Auditing Standards No. 1, *Codification of Auditing Standards and Procedures, AICPA*, Professional Standards.
3. *National Commission on Fraudulent Financial Reporting*, Report of the National Commission on Fraudulent Financial Reporting (1987).
4. *Internal Control—Integrated Framework*, www.coso.org/publications.htm Note: This reference is for the COSO internal controls report, which can be ordered through the AICPA at www.cpa2biz.com.
5. AICPA-published COSO internal control standards are described in the Statement on Auditing Standards (SAS) numbers 103, 105, 106, 107, 109, 110, and 112.
6. See Robert Moeller, *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008).
7. COSO, *Guidance on Monitoring Internal Control Systems* (2009). www.coso.org/documents/COSO_Guidance_On_Monitoring_Intro_online1.pdf.
8. Here we are presenting only a high-level summary of SOx requirements. See Moeller, *Sarbanes-Oxley Internal Controls*, for much more information.
9. As a public document, the text of the law can be found in many Web locations. One source is http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.