

**FRAUD-RELATED  
INTERNAL CONTROLS:  
COMPLYING WITH SARBANES-OXLEY  
AND SAS NO. 99**

(No. 01-5409)

**CHAPTER 1**  
**THE NEED FOR INTERNAL CONTROLS**

Many authorities on fraud believe that the most important thing an organization can do to deter most types of fraud is to design an internal control system that makes it difficult for fraud to be committed and remain undetected – and more important – that the internal control system is enforced. Internal controls help ensure the accuracy, integrity, and safety of system resources. Many security consultants jokingly refer to a new “arms race” — although in this case, the race is between those attempting to protect systems from fraud and abuse and those trying to compromise them.

The technology “arms race” is further complicated by the ever-changing landscape of information technology. For example, mainframe computers have been around long enough that companies have figured out how to protect them from fraud and abuse. As business has moved to the client/server model, the controls to protect these new systems have developed at a much slower pace than the technology itself. By the time these control issues had been resolved; the world had moved on to the Internet and embraced electronic commerce. Unfortunately, a lag often exists between technological advances and the control structures needed to keep the system honest. Dishonest people capitalize on that time lag to perpetrate fraud and otherwise damage an organization.

This course discusses how companies can develop strong systems of internal controls and presents important fraud prevention techniques.

**Threats to an Organization’s Information Systems**

Businesses have become increasingly dependent on their accounting and information systems, which have grown increasingly more complex in order to meet the escalating need for information. At the same time, companies face the growing risk of their systems being compromised, as illustrated by Table 1.1 on the next page.

**Table 1.1: Threats Faced by Organizations**

Threat	Examples
Natural and political disasters	<p>Unrelenting rains caused the Mississippi and Missouri Rivers to flood parts of eight states. Many organizations lost their computer systems, including Des Moines, Iowa, where computers were buried by 8 feet of water.</p> <p>A Los Angeles earthquake destroyed systems and others were damaged by falling debris, water from ruptured sprinkler systems, and dust.</p> <p>Fire, excessive heat, and high winds.</p>
System failures	<p>Bugs in a new tax accounting system were to blame for the State of California's failure to collect \$635 million in business taxes.</p> <p>At the Bank of New York, a field used to count the number of transactions was too small to handle the volume on a busy day. The error shut the system down and left the bank \$23 million short when it tried to close its books.</p> <p>Hardware failures, power outages, and undetected data transmission errors.</p>
Errors and Omissions; Unintentional acts	<p>A data entry clerk at Giant Food mistakenly keyed in a quarterly dividend of \$2.50 instead of \$0.25. The company paid \$10 million in excess dividends.</p> <p>A bank programmer mistakenly calculated interest for each month using 31 days. Within five months, over \$100,000 in excess interest was paid.</p> <p>Accidents caused by human carelessness, failure to follow established procedures, and poorly trained or supervised personnel.</p> <p>Lost or misplaced data and systems that do not meet company needs.</p>
Fraud	<p>A manager at a Florida newspaper went to work for a competitor when he was fired. Before long, the first employer realized that its reporters were constantly being scooped. The newspaper finally discovered that the manager still had an active account and password and regularly browsed its computer files for information on exclusive stories.</p> <p>A technology enthusiast, John Draper, discovered that the whistle offered as a prize in <i>Cap'n Crunch</i> cereal exactly duplicated the frequency of a WATS line. He used his discovery to defraud the phone companies by making numerous free telephone calls.</p>

### Why Threats Are Increasing

As a result of problems like these, controlling the security and integrity of computer systems has become a very important issue. Many organizations indicate that control risks have increased in the last few years. For example, a study conducted by Coopers & Lybrand found that more than 60% of organizations in the United Kingdom had experienced major control failure in the past two years. Studies conducted in other countries have produced similar statistics. Among the many reasons for the increase in security problems are these:

- Increasing numbers of client/server systems means that information is available to an unprecedented number of workers. Computers and servers are everywhere: there are PCs on most desktops, and portables accompany people wherever they go.
- Because local area networks (LANs) and client/server systems distribute data to many users, they are harder to control than centralized, mainframe systems. At Chevron, for instance, information is distributed among many systems and thousands of employees working locally and remotely, as well as nationally and internationally.
- Wide area networks (WANs) are giving customers and suppliers access to each other's systems and data, making confidentiality a major concern. For example, Wal-Mart allows Procter & Gamble (P&G) to have access to certain information in its computers as a condition of their alliance. Imagine the potential confidentiality problems as P&G also forms alliances with Wal-Mart competitors such as Kmart and Target Stores.

Unfortunately, many organizations do not adequately protect their data due to one or more of the following reasons:

- Computer control problems are often underestimated and downplayed, and companies view the loss of crucial information as a distant, unlikely threat.
- Control implications of moving from the centralized, host-based computer systems of the past to those of a networked system are not fully understood.
- Many companies do not realize that data security is crucial to their survival. Information is a strategic resource, and protecting it, therefore, should be a strategic requirement. For example, one company lost millions of dollars over a period of several years because it did not protect its data transmissions. A competitor tapped into its phone lines and obtained faxes of new product designs

being sent to an offshore plant.

- Productivity and cost pressures motivate management to forgo time-consuming control measures.

### **Designing Internal Control Systems to Curb the Threats**

Fortunately, companies are increasingly recognizing the problems and taking positive steps to tighten internal control and security. For example, many are becoming proactive in their approach, devoting full-time staff to security and control concerns and educating their employees about control measures. Others are establishing and enforcing formal information security policies by making controls a part of the applications development process and moving sensitive data off unsecured client servers to a more secure environment, such as a mainframes.

The overall responsibility for a secure and adequately controlled system lies with top management. Managers typically delegate the design of adequate control systems to systems analysts, designers, and end users. The corporate information security officer and the operations staff are typically responsible for ensuring that control procedures are followed.

Achieving adequate security and control over the information resources of an organization should be a top management priority. Although internal control objectives remain the same regardless of the data processing method, a computer-based information system requires different internal control policies and procedures. For example, while computer processing reduces the potential for clerical errors, it may increase the risks of unauthorized access to or modification of data files. In addition, segregating the authorization, recording and asset custody functions within an information system must be achieved differently, since computer programs are likely responsible for two or all three of these functions. Fortunately, computers also provide opportunities for an organization to enhance its internal controls.

Assisting management in the control of a business organization is one of the primary objectives of an information system. Managers, system designers, and accountants can help achieve this objective by designing effective control systems and by auditing (or reviewing) control systems already in place to assure that they are operating effectively.

It is especially important to ensure that internal controls are in place at the end of the year during holiday season. Research shows that a disproportionate amount of computer fraud and security breaches take place during holidays. Some reasons for this are extended employee vacations (hence fewer people to “mind the store”), students are out of school and have more time on their hands, and counterculture hackers take advantage of holidays, thus increasing their attacks on systems.

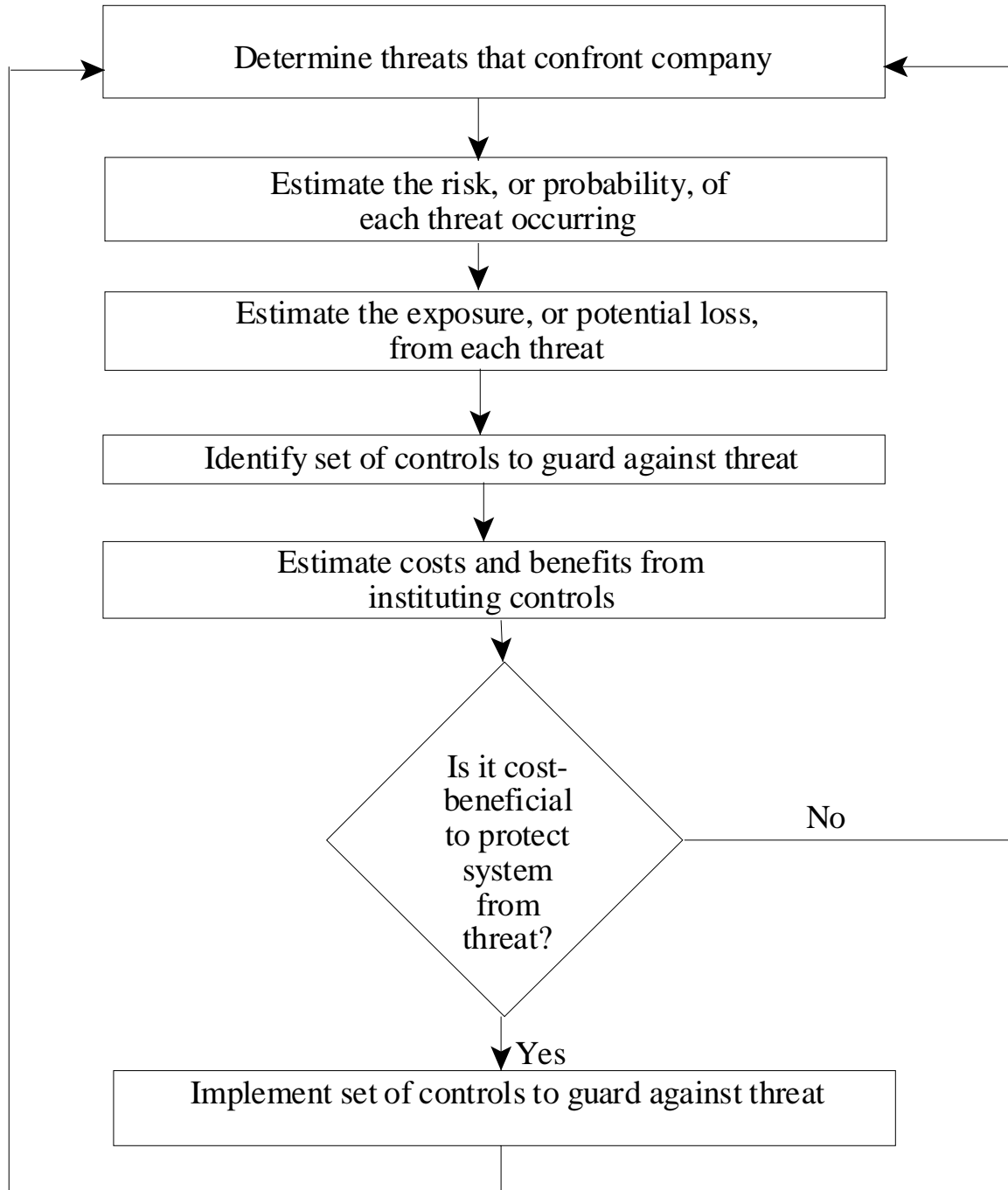
Any potential adverse occurrence or unwanted event that could be injurious to either an information system or the organization, such as one or more of these elements, is referred to as a *threat*. The potential dollar loss, should a particular threat become a reality, is referred to as the *exposure* from the threat, and the likelihood that the threat will actually come to pass is referred to as the *risk* associated with the threat.

It is important to understand how to protect systems from threats. Management expects accountants to be their “control consultants.” That is, management considers it to be their responsibility to: (1) take a proactive approach to eliminating system threats, and (2) detect, correct, and recover from threats if and when they occur.

To develop efficient, cost-effective controls, designers should follow the risk assessment strategy presented in Figure 1.1 and explained in detail in Chapter 2. These controls are much more effective when implemented as the system is built, rather than as an afterthought. Management must also establish procedures to ensure that the controls are complied with and enforced.

Our focus in this course is on controls designed to prevent and detect frauds; however, the control methods discussed in the course will serve to protect the system from most all threats that an organization and its information system will face.

Figure 1.1 Risk Assessment Approach to Designing Internal Controls



### **Overview of Control Concepts**

Internal control is the organizational plan and methods a business uses to safeguard assets, provide accurate and reliable information, promote and improve operational efficiency, and encourage adherence to prescribed managerial policies — purposes that are often at odds with one another. For example, people may push for radical business process re-engineering in order to get better and faster information and improve operational efficiency. Others may resist such changes because they compromise the safety of company assets and require significant managerial policy changes.

Management control is broader than internal accounting control, and it encompasses the following three features: (1) it is an integral part of management responsibilities; (2) it is designed to reduce errors and irregularities and achieve organizational goals; and (3) it is personnel-oriented and seeks to help employees attain company goals by following organizational policies.

The internal control structure consists of the policies and procedures established to provide a reasonable level of assurance that the organization's specific objectives will be achieved. The system only provides reasonable assurance because a system that provides complete assurance would be difficult to design and prohibitively expensive.

### **Internal Control Classifications**

The concepts of internal control and management control are broad in scope and aimed at describing entire control systems. The specific control procedures used in these systems may be classified using the following four internal control categories.

#### **Preventive, Detective, and Corrective**

Preventive controls deter problems before they arise. Hiring highly qualified accounting personnel, appropriately segregating employee duties, and effectively controlling physical access to assets, facilities and information are effective preventive controls. Because not all control problems can be prevented, detective controls are needed to discover control problems as soon as they arise. Examples of detective controls are duplicate checking of calculations as well as reconciling bank records and monthly trial balances. Corrective controls remedy problems discovered with detective controls. They include procedures implemented to: (1) identify the cause of a problem, (2) correct resulting errors or difficulties, and (3) modify the system so that future problems are minimized or eliminated. Examples include maintaining back-up copies of key transactions and master files and adhering to data entry correction procedures, as well as procedures for resubmitting transactions for processing.

### **General and Application**

General controls are designed to ensure that an organization's control environment remains stable and well managed in order to enhance the effectiveness of application controls. Application controls are used to prevent, detect, and correct errors and irregularities in transactions as they are processed. These are considered in depth in Chapters 3 and 4.

### **Administrative and Accounting**

Administrative controls help ensure operational efficiency and adherence to managerial policies. In contrast, accounting controls help safeguard assets and ensure the reliability of financial records.

### **Input, Processing, Data Storage, and Output**

Controls can also be classified according to where they are implemented in the data processing cycle. Input controls are designed to ensure that only accurate, valid, and authorized data are entered into the system. For example, the computer could be programmed to reject payroll input for employees unless they are included on a list of authorized employees. Processing controls are designed to ensure that all transactions are processed accurately and completely and that all files and records are properly updated. An example is the batch totals described later. Data storage controls ensure that stored data is not lost, corrupted, or misused. For example, storing a back-up copy of critical data files helps companies recover from damage to their computer systems. Output controls are designed to ensure that system output is properly controlled. For example, unauthorized employees should be prevented from obtaining a copy of the report documenting top management's salaries.

The nature of a particular control procedure is less important than whether it effectively accomplishes its objective, which is to prevent organizational losses due to a particular threat or hazard. In analyzing controls, it is important first to define an organization's control objectives. The next step is to determine whether or not effective control procedures are in place to accomplish these control objectives.

### **The Foreign Corrupt Practices Act**

In 1977, shock waves reverberated through the accounting profession when Congress incorporated language from an AICPA pronouncement into the Foreign Corrupt Practices Act. Specifically, all publicly-owned corporations subject to the Securities Exchange Act of 1934 are now legally required to keep records that accurately and fairly reflect their transactions and assets in reasonable detail. They must also devise and maintain an internal accounting control system sufficient to provide reasonable assurances that: (1) transactions are properly authorized and recorded; (2) assets are safeguarded and

protected from unauthorized access; and (3) recorded asset values are periodically compared with actual assets, and any differences are corrected.

The primary purpose of the Act was to prevent the bribery of foreign officials in order to obtain business. A significant effect of the Act, however, was to require corporations to maintain good systems of internal accounting control. Needless to say, this requirement has generated tremendous interest among management, accountants and auditors in the design and evaluation of internal control systems. It is important to recognize that it is much easier to build controls into a system at the initial design stage than to add them after the system has been built. For that reason, accountants and other control experts should be important members of the team that develops or modifies an information system.

### **The Sarbanes-Oxley Act**

The airwaves and printed pages in the late 1990s and early 2000s were full of news of accounting frauds and problems at Enron, WorldCom, Xerox, Global Crossing, Adelphia, and Qwest. When Enron, with \$62 billion in assets, declared bankruptcy in December 2001 it was the largest bankruptcy in U.S. history. In June, 2002 Arthur Andersen, once the largest of the Big 5 CPA firms, collapsed. The Enron bankruptcy was dwarfed when WorldCom, with over \$100 billion in assets, filed for bankruptcy in July, 2002.

In response to these problems, Congress passed the Sarbanes-Oxley Act of 2002 (SOX), also known as the Corporate and Criminal Fraud Accountability Act. President Bush signed SOX into law on July 30, 2002. SOX, which applies to publicly held companies and their auditors, was intended to prevent financial statement fraud, make financial reports more transparent, provide protection to investors, strengthen the internal controls at public companies and punish executives who perpetrate fraud.

SOX has had a material impact on the way boards of directors, management, and accountants of publicly held companies operate. It has also had a dramatic impact on CPAs of publicly held companies and the audits of those companies. Since the enactment of Sarbanes-Oxley, the Securities and Exchange Commission (SEC) has issued numerous SEC Releases that support and expand the Act's requirements. Below is a summary of some of the most important provisions of Sarbanes-Oxley and the corresponding SEC Releases that relate to fraud detection and prevention.

### **Public Company Accounting Oversight Board**

SOX created a five member Public Company Accounting Oversight Board (PCAOB) to regulate and provide oversight to the accounting profession. The SEC appoints five full-time, financially-literate members of the PCAOB and oversees their activities. PCAOB members serve five-year staggered terms, and during their time of service they cannot have any other employment.

In effect, the auditing profession is now regulated by non-accountants, as three of the PCAOB members must not be and cannot have been CPAs. The remaining two members must be or must have been CPAs. The Chair may be either a CPA member or a non-CPA member. If a CPA member, the chair must not have practiced accounting during the five years preceding his/her appointment. PCAOB members may not receive payments from, or share in any of the profits of, any public accounting firms except for “fixed continuing payments,” such as retirement payments.

The PCAOB is funded by mandatory fees imposed on public companies as well as registration and annual fees from firms that audit public companies. All auditing firms who audit public companies must register with the PCAOB. Each accountant and firm who registers must agree to cooperate with any investigation the PCAOB performs. Those who violate the agreement face suspension.

The PCAOB was given the power and the responsibility to set, establish, adopt and enforce auditing and related attestation, quality control, ethics, independence and other standards relating to the preparation of audit reports that are necessary to protect the public interest. The PCAOB will continue to recognize Financial Accounting Standards Board (FASB) statements as being generally accepted. The PCAOB will also perform inspections of the quality controls at audit firms under its oversight.

The PCAOB was also given the responsibility and power to:

- Register public accounting firms.
- Make an annual report to the SEC on its standard-setting activities.
- Conduct inspections of registered accounting firms. Large registered accounting firms will be investigated every year, smaller ones every three years. The purpose of the inspection is to assess the company’s compliance with their own quality control policies, SEC and PCAOB rules, and professional standards. Violations can result in disciplinary action by the PCAOB and can also be reported to the SEC and the state boards of accountancy.
- Investigate potential violations of securities laws, standards, competency, and conduct, and discipline fraudulent auditors and company executives. While conducting an investigation, the PCAOB can require the registered accounting firm to provide testimony or documents and can also request information from relevant outsiders. The PCAOB has the power to refer investigations to the SEC and, with SEC approval, to the Department of Justice, state attorneys general or state boards of accountancy.
- Sanction firms and individuals for violations of laws, regulations, and rules for failure to supervise a partner or employee in a registered accounting firm and for not cooperating with investigations. Sanctions include revocation or suspension of an accounting firm’s registration, prohibition from auditing public companies, suspension of auditors from working for public companies, and imposition of civil penalties on individual auditors and on accounting firms.

- Enforce compliance with the SOX Act, PCAOB rules, professional standards, and the securities laws that govern how audit reports are prepared and issued and the obligations and liabilities of accountants with respect thereto.
- Adopt an audit standard to implement the internal control review required by section 404 of SOX. This standard requires the auditor to: a) evaluate whether a company's internal control structure and procedures include records that accurately and fairly reflect their transactions, b) provide reasonable assurance that the transactions are recorded such that financial statements can be prepared in accordance with GAAP, and c) describe any material internal control weaknesses.
- Perform any other function or duty they consider appropriate or necessary.

### **New Rules for Auditors**

The following SOX provisions affect accounting firms and their public company audits:

- Auditors must report to the audit committee certain critical information, including:
  - Critical accounting policies and practices the company uses.
  - The alternative GAAP treatments of financial information discussed with management, the ramifications of the alternative disclosures and treatments, and the preferred treatment.
  - Any and all accounting disagreements between the auditor and management.
  - Other relevant communications between the auditor and management.
- All public company audit reports must have a thorough second partner review and approval.
- The lead and review audit partners have to be rotated every five years and may not return to the audit for five years. Audit partners with significant client involvement must rotate after seven years and wait two years before returning to the audit.
- All publicly held companies must issue a report to accompany the financial statements that contains management's assessment of the company's internal controls. Auditors must evaluate management's assessment of internal control structures and attest to its accuracy, including a specific notation about any significant defects or material noncompliance found during their internal control tests.
- SOX makes it unlawful for auditors to provide the following non-audit services to their publicly held audit clients:
  - Bookkeeping or other accounting records or financial statement services.
  - Financial information systems design and implementation.
  - Appraisal or valuation services, fairness opinions, or contribution-in-kind reports.
  - Actuarial services.
  - Internal audit outsourcing services.
  - Management functions or human resource services.
  - Broker, dealer, investment adviser, or investment banking services.
  - Legal services and expert services unrelated to audit services.
- SOX has a catch-all category that authorizes the PCAOB to prohibit any other service it deems appropriate. The SEC has three guiding principles for deciding whether other services can be

performed: the auditor cannot perform a management function, audit his or her own work, or serve as a client advocate.

- The PCAOB can exempt a person, financial statement issuer, public accounting firm or transaction, from these prohibitions with SEC approval.
- Non-audit services not banned by SOX, such as tax services, are allowed if pre-approved by the company's audit committee. However, the SEC has indicated that certain tax services could impair auditor independence, particularly tax shelter recommendations that have tax avoidance as their sole or primary purpose and may not be supported by IRS code. In essence, the auditor would not be independent because they would be evaluating the tax shelter consequences of their own recommendations.
- The authority to pre-approve services can be delegated to one or more audit committee members if the decision is presented to the full audit committee. The pre-approval of non-audit services requirement can be waived in a very limited number of instances.
- All pre-approved non-audit services have to be disclosed to investors in periodic reports.
- Accountings firm can not provide audit services to a company if a top official (CEO, Controller, CFO, Chief Accounting Officer, etc.) was employed by the accounting firm and worked on the public company's audit during the 12-month period preceding the audit. Auditors can accept positions such as assistant controller or accountant without violating this new requirement.
- CPA firms must prepare audit work papers and other audit report information in sufficient detail to support their conclusions and maintain the documentation for at least 7 years. After SOX was passed, the SEC passed record retention rules that significantly increase the documentation that must be retained. Auditors must also retain correspondence, communications and other documents and records (including electronic ones such as e-mail) that contain conclusions, opinions, analyses, or financial data and were created, sent or received in connection with the audit or review.

### **New Roles for Audit Committees**

SOX gave audit committees more power and responsibility over a company's auditors. The intent of these new rules is to make the audit committee the auditor's "client," rather than company management. Companies can be delisted from the stock exchanges if they fail to comply with the new rules.

SOX requires that:

- Auditor's report to be overseen by a company's audit committee, not management.
- Audit committees to be responsible for hiring, compensating, and overseeing registered public accounting firms they employ and hiring independent counsel and any other advisors they determine necessary.
- Each person on the audit committee be a member of the board of directors and be otherwise

independent of the company. SOX defined independent as not receiving any other compensation from the company and not being affiliated with the company or any of its subsidiaries.

- One member of the audit committee must be a financial expert. A company without a financial expert must disclose that fact and explain its rationale. The SEC has defined a financial expert as someone with:
  - An understanding of GAAP and financial statements.
  - The ability to assess whether GAAP was used in estimates, accruals, and reserves.
  - Experience with financial statements of a similar breadth and complexity of issues.
  - An understanding of internal controls and financial reporting procedures.
  - An understanding of audit committee functions.
  - The New York Stock Exchange requires the chair of the audit committee to have accounting or financial management experience. They also require a nominating committee and a compensation committee composed of independent directors.
- Companies provide appropriate funding to its audit committee.
- Audit committees pre-approve all audit and non-audit services provided by its auditor that are not specifically prohibited by SOX.
- Audit committees set up procedures to receive and deal with any complaints the company receives about accounting, internal control, auditing, and similar issues.

### **New Rules for Management**

Perhaps the biggest change SOX mandates for management of public companies is more responsibility for financial reports filed with the SEC. SOX requires both the CEO and CFO to prepare a statement to accompany the audit report that certifies their quarterly and annual financial statements and disclosures. There are six elements to the management certification:

1. The financial statements have been reviewed by management.
2. The statements do not contain an untrue statement of a material fact or omit a material fact that makes the statement misleading.
3. The statements fairly present, in all material respects, the operations, financial condition and cash flow of the issuer.
4. Management is responsible for designing, installing, and evaluating disclosure controls and procedures and reporting their conclusions with respect to their effectiveness.
5. All material internal control weaknesses and fraud are disclosed to the auditor.
6. All significant changes to internal controls after management's evaluation have been disclosed and corrected.

These rules were implemented to ensure investors that the information in a company's quarterly and annual reports is accurate and contain all of the company information that the executives believe is important to a reasonable investor.

If management willfully and knowingly violates this certification process, they can be punished with imprisonment of up to 20 years and a fine of up to \$5,000,000. In addition, if financial reports must be restated due to material noncompliance with financial reporting requirements, a violation of securities laws, or securities fraud, company management can be required to repay bonuses and incentive or equity-based compensation they realized during the twelve months following the issuance or filing of the noncompliant document. They can also be required to repay any profits they realized from the sale of company securities during the same period.

As a result of these new certification requirements, many public company CEOs and CFOs are spending a great deal of time conducting due diligence procedures on their financial statements before certifying them.

SOX also set forth the following new rules for company management:

- Company officers and directors can not take any action to fraudulently influence, coerce, manipulate, or mislead auditors to make the financial statements materially misleading.
- Company executives and directors can not receive loans that are unavailable to those outside the company. There is an exception for loans, such as a home mortgage or a credit card agreement, if they are on the same terms and conditions as those made to the general public and done in the ordinary course of business.
- Company executives and directors can not trade company stock during blackout periods when other employees are unable to do so. Profits from doing so can be recovered.
- All insider stock trades involving executives and individuals who own 10 percent or more of the company must be reported electronically to the SEC within two days and posted to the companies' websites.
- All financial reports required by GAAP must contain all material correcting adjustments identified by the auditors.
- All annual and quarterly financial reports must disclose all material off-balance sheet transactions and relationships with unconsolidated entities likely to have a material effect on the company's financial condition.
- Pro forma financial information must not contain any untrue statements or omit a material fact that would make it misleading and should be in conformance with company financial information prepared according to GAAP.
- Companies must disclose, in plain English, material changes to their financial condition on a rapid and current basis.

### **Management Assessment of Internal Controls Requirement**

SOX requires management of public companies to include in its annual report an internal control report that:

- States management is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting.
- Assesses the effectiveness of the company's internal control structure and financial reporting procedures as of the end of the company's fiscal year.

SOX also specifies that a company's auditor must attest to as well as report on management's internal control assessment. Each audit report must describe the scope of the auditor's internal control structure tests.

SOX requires executives to establish and maintain controls and procedures to ensure they are informed of all important company information and to alert their auditors and board of directors of any control weaknesses or problems.

After SOX was passed, the SEC defined financial reporting internal controls as a process designed by or under the direction of the CEO and the CFO to provide reasonable assurance that financial reporting is reliable, and that external financial statements were prepared in accordance with GAAP and include policies and procedures to provide reasonable assurance that:

- Records are maintained in sufficient detail to accurately and fairly reflect company assets.
- The unauthorized acquisition, use, or disposition of material company assets is prevented or detected on a timely basis.
- Company transactions are recorded such that financial statements can be prepared in accordance with GAAP.
- Company receipts and expenditures are made in accordance with management and directors authorizations.

In addition, the SEC has mandated that:

- Management must base its evaluation on a recognized control framework developed using a due-process procedure that allows for public comment. The most likely framework is the one formulated by COSO (Committee on Sponsoring Organizations).
- The report must contain a statement identifying the framework used by management to evaluate internal control effectiveness.
- Management must disclose any and all material internal control weaknesses.
- Management can not conclude that the company has effective internal control over financial reporting if there are any material weaknesses.

(Internal control over financial reporting and management's assessment thereof are discussed in greater detail later in this chapter.)

### **Powers Granted to the SEC**

SOX gives the SEC the following powers and responsibilities:

- Oversee the activities and functions of the PCAOB and, if needed, give it additional responsibilities.
- Inspect the PCAOB.
- Review and approve PCAOB standards and rules and amend them if they see fit.
- Modify, enhance, reduce, or rescind PCAOB sanctions or penalties.
- Censure or impose limitations upon the activities, functions, and operations of the PCAOB if it violates federal law or fails to make sure accounting firms comply with applicable rules without reasonable justification.
- Freeze extraordinary payments to directors, offices, partners, controlling persons, agents, or employees during an investigation of possible securities laws violations.
- Prohibit a person from serving as an officer or director of a public company if the person has committed securities fraud or is found to be unfit.
- Issue rules to require financial statement issuers to disclose whether at least 1 member of its audit committee is a financial expert.
- Require companies to disclose whether they have adopted a code of ethics for senior financial officers (CEO, CFO, controller, etc.) and the contents of that code or disclose why they failed to do so.

### **New Criminal Penalties**

SOX and the SEC rules implementing its requirements increase the maximum penalties for many white-collar crimes and create tough penalties for people who destroy records, commit securities fraud, and fail to report fraud. CPA firms are required to preserve all audit or review work papers, including e-mail, for at least seven years after the audit is complete. Willfully failing to do so or intentionally destroying these records is now a felony, with penalties of up to 10 years incarceration.

The law creates a new felony, with penalties of up to 20 years and a hefty fine, for destroying, altering or fabricating documents to impede, obstruct or influence any existing or contemplated federal investigation. The criminal penalty for securities fraud was increased to 25 years. The statute of limitations on securities fraud claims was extended from one to two years from the date the fraud is discovered, and from three to five years after the fraud took place.

The law increases the penalty for CEOs and CFOs who knowingly certify fraudulent financial statements or submit materially misleading statements to the SEC to a maximum of 10 years and a \$1

million fine. CEOs and CFOs who willingly do so will face a maximum penalty of 20 years and a \$5 million fine.

### **Foreign Public Accounting Firms**

Foreign accounting firms that prepare or furnish audit reports of U.S. companies must register with the PCAOB and be subject to their authority, including firms that perform some audit work, such as in a foreign subsidiary of a U.S. company that is relied on by the primary auditor. If a registered U.S. accounting firm relies on the opinion of a foreign accounting firm, their audit work papers must be supplied upon request to the PCAOB or the SEC.

### **Whistleblower Protection**

In an effort to encourage people to report fraud and to help the government prosecute those who commit fraud, SOX included provisions that expand the rights of whistleblowers. As a result of the new law, employers are prohibited from taking action against employees who lawfully blow the whistle on fraud. SOX also make it possible for employees to sue their employers for compensatory damages if the employers retaliate against them.

### **Consideration by Appropriate State Regulatory Authorities**

SOX direct state regulators to determine whether PCAOB standards should be applied to small and mid-size non-registered accounting firms. This possible cascade effect of SOX is of particular concern to small businesses and accounting firms. In a number of states, SOX is being used to develop parallel federal and state laws or rule changes that directly affect both non-public companies and the CPAs that provide services to them

## **Internal Control over Financial Reporting**

While the scope of the Sarbanes-Oxley Act is far-reaching, perhaps its most significant provision is the enhancement of management's responsibilities pertaining to internal controls. Under Section 404 of the Act, SEC Release Nos. 33-8238 and 34-47986, and PCAOB Auditing Standard No. 2, management must evaluate and report on the effectiveness of the company's system of internal control over financial reporting.

### **Defining Internal Control over Financial Reporting**

The SEC defines internal control over financial reporting (ICOFR) as:

*“A process designed ...to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles...”*

Additionally, ICFR is deemed to include all policies and procedures that:

*“Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the [company];*

- *Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the [company] are being made only in accordance with authorizations of management and directors of the [company]; and*
- *Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the [company’s] assets that could have a material effect on the financial statements.”*

Additionally, ICFR is deemed to include all policies and procedures that:

- “Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the [company];
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the [company] are being made only in accordance with authorizations of management and directors of the [company]; and
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the [company’s] assets that could have a material effect on the financial statements.”

Examples of internal controls covered by Section 404 and the related SEC Releases and PCAOB Standard include, but are not limited to:

- Controls over initiating, authorizing, recording, processing, reconciling and reporting significant account balances, transactions and disclosures included in the financial statements.
- Controls related to the prevention, identification, and detection of fraud.
- Controls related to initiating and processing of non-routing and non-systematic transactions.
- Controls related to the selection and application of appropriate accounting policies.

### **Management’s Report on Internal Control**

The provisions of Section 404 require management to acknowledge its responsibility for the ICFR of the company and to assess the operating effectiveness of those controls. As a result, public companies must issue an additional internal control report within their annual report containing:

- A statement of management’s responsibility for establishing and maintaining adequate ICFR;
- A statement identifying the framework that management used in conducting the assessment of the effectiveness of the company’s ICFR;
- Management’s assessment of the effectiveness of the company’s ICFR as of the end of the

company's most recent fiscal year, including disclosure of any material weaknesses identified in the company's ICOFR and an explicit statement as to whether the or not the ICOFR is effective; and

- A statement that the company's independent auditor has issued an attestation report covering management's assessment of the company's ICOFR. The auditor's attestation report must also be filed with the annual report.

### **Management's Assessment of Internal Control**

In performing the ICOFR assessment, management must choose a suitable internal control framework against which to evaluate the design and effectiveness of the company's ICOFR. The most commonly used model in the United States is the Internal Control — Integrated Framework established by the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission, which provides five components of effective internal controls:

- Control Environment
- Control Activities
- Risk Assessment
- Information and Communication
- Monitoring

Additionally, management must:

- Determine which internal controls to test in performing the assessment, considering the significance of each control, both individually and in the aggregate;
- Evaluate whether the failure of a control could result in a misstatement to the financial statements, the likelihood and magnitude of any resulting misstatement, and whether other controls are in place to mitigate this occurrence;
- Determine which locations or business units to include in the assessment, if applicable;
- Evaluate the design and operating effectiveness of the internal controls using the internal control framework chosen as a guide;
- Evaluate the probability of occurrence and the size of potential misstatements resulting from the internal control deficiencies identified and determine whether they, either individually or in the aggregate, constitute material weaknesses (any deficiency where the likelihood of potential misstatement is more than remote) or significant deficiencies (any deficiency where the likelihood of potential misstatement is more than remote and the magnitude is more than inconsequential);
- Provide sufficient documentation to support the assessment of ICOFR, including documenting the design of the internal controls and the results of management's testing and evaluation; and
- Communicate the assessment findings to the independent auditor and any other applicable parties.