CHAPTER 7

Corporate Information Security and Privacy Regulation

THIS CHAPTER FOCUSES ON SPECIAL SECURITY ISSUES faced by publicly traded companies. Public companies must comply with a law that tries to improve corporate responsibility and stop fraudulent financial reporting. Rules and regulations created in response to the law impact information systems that process financial data. The rules require that these systems be reviewed to make sure that they appropriately control information security risks and threats to financial data.

This chapter reviews why Congress created this law. It also reviews how the law influences information security practices. Finally, it discusses how this law affects other kinds of organizations.

Chapter 7 Topics

This chapter covers the following topics and concepts:

- How the Enron scandal led to securities-law reform
- Why accurate financial reporting is important
- What the Sarbanes-Oxley Act (SOX) is
- What compliance and security controls are
- How SOX influences other types of companies
- What some corporate privacy issues are
- What some case studies and examples are

Chapter 7 Goals

When you complete this chapter, you will be able to:

- Describe the difference between public and private companies
- Explain the history behind the Sarbanes-Oxley Act
- Discuss the main requirements of the Sarbanes-Oxley Act
- Explain the role of the Public Company Accounting Oversight Board
- Describe how Section 404 internal control requirements impact information security
- Discuss frameworks used to guide Sarbanes-Oxley internal control requirements

The Enron Scandal and Securities-Law Reform

Enron. WorldCom. Tyco. Adelphia. These companies have come to represent a wave of corporate scandal that plagued America in the early 2000s. Each company engaged in varying levels of mismanagement, questionable financial deals, and accounting fraud. The activities at these companies shook investor confidence in U.S. corporations. They also tarnished the reputations of financial services professionals such as analysts, accountants, and auditors. Consider the following:

- Once called the "Most Innovative Company in America," energy company Enron filed for bankruptcy in December 2001. It used a number of different fraudulent accounting methods to hide billions of dollars of debt from its investors and lenders.
- Cable company Adelphia filed for bankruptcy in June 2002. In 2004, a federal jury convicted Adelphia's founder of bank and securities fraud. He was sentenced to 15 years in prison.
- Telecommunications company WorldCom filed for bankruptcy in July 2002. At the time, it was the largest bankruptcy in U.S. history. In July 2005, a federal court sentenced the chief executive officer (CEO) of WorldCom to 25 years in prison for corporate fraud.
- In June 2005, a jury convicted a former Tyco CEO of theft, conspiracy, securities fraud, and falsifying business records. A court in New York sentenced him to between eight and 25 years in prison. He was ordered to pay restitution and fines of more $200 million.

The financial mismanagement at these companies contributed to the largest reform in U.S. securities laws since the Great Depression. The Enron bankruptcy is the case that spurred Congress to act. It's important to understand the Enron scandal to appreciate how significant the reform was.

Public Versus Private Companies

A **public company** also is called a publicly traded company. Many investors own a public company. The investors own a portion of the company in the form of stock. A stock represents a share of a corporation's profits or assets. A person's percentage of ownership in the corporation depends on how many shares of stock he or she owns.

Shareholders are entitled to portions of a public company's profits. Their share is called a **dividend**. A dividend represents the shareholder's portion of the company's earnings. People who own more shares of stock receive larger dividends.

Public corporations are allowed to sell stocks and bonds. A bond represents a loan to the corporation for a specified period. The corporation must pay bondholders back the full value of the bond, plus interest. A person who owns a corporate bond doesn't have any ownership in a corporation. Only stocks represent an ownership interest. Stocks and bonds together are called **securities**.

In the U.S., the stock of a public company is traded on a stock exchange. The two most popular U.S. stock exchanges are the New York Stock Exchange (NYSE) and the NASDAQ Stock Market. National securities exchanges are registered with the U.S. Securities and Exchange Commission (SEC). You can learn more at *http://www.sec.gov/divisions/marketreg/mrexchanges.shtml*.

Almost all securities sold in the United States must be registered with the SEC. To register its securities, a company must file documents about its financial condition with the SEC. It must file these documents with the SEC on a regular basis. Investors review these documents to make informed investment decisions.

A public company is different from a **privately held company**. A small group of private investors owns a privately held company. In some cases, the investors all might be members of the same family. A private company doesn't have to answer to shareholders in the same way that a public company does. A private company distributes its profits to its owners.

Private companies don't have to register with the SEC. They also don't have to file documents with the SEC that show their financial position. The largest private companies in the United States include Cargill, Koch Industries, Dell, and Mars.[1] Dell joined the list in 2013. It was a public company for several years. It became a private company again when its founder purchased all shares of Dell stock.

Corporate Fraud at Enron

The Enron case has become a part of American pop culture. Its name is synonymous with corporate greed and scandal. More than 10 years after the scandal, it continues to hold our attention. CNBC aired a documentary in April 2010 called "Enron: The Smartest Guys in the Room."[2] The Enron scandal inspired a musical called "Enron: The Musical." The musical played on Broadway for a couple of months in 2010.[3]

Enron formed in 1985 through the merger of two natural gas companies. It was based in Houston, Texas. Kenneth Lay was the CEO of the company. By the mid 1990s, Enron was the leading U.S. natural gas company.

Enron grew quickly because it took advantage of energy market deregulation in the late 1980s. It bought and sold gas and electricity. It did this through futures contracts. These investments were initially very successful. As it grew, Enron expanded into other markets. It purchased steel mills, water utilities, and even tried to enter the Internet broadband market. It also expanded internationally, pursuing opportunities in England, Mexico, and India.

From 1997 to 2001, *Fortune* magazine put Enron on its "Most Innovative Companies in America" list.[4] In 2000, it named Enron to its "World's Most Admired Companies" list.[5] Enron grew from 7,500 employees in 1996 to more than 20,000 employees in 2001. Its stock was valuable. Enron encouraged its employees to include Enron stock in their retirement portfolios.

To the outside world, Enron was a very successful company. Its required filings with the U.S. Securities and Exchange Commission (SEC) showed that it was making money. It appeared to be able to translate its success in the energy markets to other markets. Financial analysts continued to recommend Enron stock. Investors continued to buy it.

In reality, Enron was struggling. It lost billions of dollars on its international investments. Enron also started to face increased competition in the energy business. It began to lose its market share in energy futures contracts. This is because other energy companies started to use Enron's own strategies to become profitable.

By the late 1990s, Enron was in financial trouble. It needed to raise money to meet its operating expenses. However, it couldn't do this in a way that would alarm its investors. It didn't want to alert investors to potential trouble. This could cause its stock price to fall. Maintaining a high stock price was important to bring in new investors. It also was critical to being able to maintain credit lines with banks.

FYI

A *futures contract* is a contract for the sale of a good. One party agrees to sell the other party an asset at some point in the future. The two parties agree on the future quantity and price for the asset at the time the contract is made. Companies use futures contracts as an investment tool rather than as an actual contract to supply goods.

Enron executives engaged in a number of complicated financial transactions to hide its losses. Its chief financial officer (CFO), Andrew Fastow, created a number of affiliated companies. He hid Enron's losses in the financial records of these companies. The Enron CFO and other employees who worked with him owned many of these affiliated companies. They profited from the transactions between Enron and the affiliated companies.

These transactions were very complex. They were complicated to understand because Enron often changed the names of its different divisions. It also moved assets back and forth between divisions. Many of these transactions violated traditional accounting principles. These principles are called generally accepted accounting principles (GAAP). They are the rules for the accounting process. Accountants prepare financial statements according to these rules. These rules are designed to promote accurate accounting records.

Enron also mislabeled loans that it received from banks. It did this to hide the transactions on its own financial statements so that its investors would not know about them. By some reports, Enron borrowed about $8.6 billion from 1992 to 2001.[6] It hid these loans from its investors. During this time, Enron filed earnings statements with the SEC that misstated its financial position. The SEC filings were hard to understand. They also showed that Enron appeared to be making money.

In February 2001, CEO Kenneth Lay retired. The new CEO was Jeffrey Skilling. Skilling had been instrumental in taking Enron into new trading markets in the 1990s. He and CFO Andrew Fastow oversaw most of Enron's business practices.

In April 2001, many financial analysts began to question Enron's complicated financial statements.[7] Enron continued to portray the image of a successful company. Jeffrey Skilling unexpectedly resigned from the CEO post in August 2001. The Board of Directors asked Kenneth Lay to return to Enron as its CEO. Lay resumed his old post.

In October 2001, Enron announced its first ever loss. The SEC noticed this announcement and began to review Enron's financial statements. Enron also began its own investigation. In late October, the Enron Board of Directors established a special committee to investigate the affiliated companies created by Fastow. Director William C. Powers led this committee. The report that the committee issued is known as the "Powers Report."[8]

In November 2001, Enron announced that it was amending its 1997–2001 financial statements because of accounting errors. This announcement shook investor confidence in Enron. Its stock price began to drop. Banks would no longer issue it credit to meet its operating expenses. At the end of November 2001, Enron stock was worth less than a dollar per share.[9]

FYI

The Powers Report was released in February 2002. It noted that Enron's executive officers mismanaged many aspects of the company's business. It also placed blame on Enron's board of directors for failing in its corporate oversight duties. It blamed Enron's accounting advisor, Arthur Andersen, for failing to provide objective accounting advice. You can read a copy of the report at *http://i.cnn.net/cnn/2002/LAW/02/02/enron.report/powers.report.pdf*.

On December 2, 2001, Enron filed for bankruptcy. At the time, it was the largest bankruptcy ever. (The WorldCom bankruptcy surpassed it only six months later.[10]) In January 2002, Enron removed its stock from the New York Stock Exchange.[11]

The fallout from the Enron case was enormous. Employees who had invested their retirement savings in Enron stock lost $1.3 billion.[12] The accounting firm Arthur Andersen, Enron's auditor, closed down. The U.S. government prosecuted many of Enron's top executives for their involvement in its business dealings. Some of these prosecutions were difficult because it was hard to determine which executives were involved in the fraud, and which executives weren't. The complexity of Enron's financial dealings contributed to this difficulty.

CFO Andrew Fastow entered into a plea agreement with the U.S. government. He agreed to testify against Jeffrey Skilling and Kenneth Lay in exchange for a sentence of no more than 10 years in prison. In September 2006, a federal court sentenced him to six years in prison. He also paid more than $30 million in restitution. Fastow was released from prison in December 2011.

Enron founder and CEO Kenneth Lay was convicted in May 2006 for fraud and conspiracy. He died of a heart attack in July 2006. The court vacated his conviction after his death. His conviction was erased because he died before he could appeal his conviction.

Former CEO Jeffrey Skilling was convicted in 2006 on federal fraud charges. A federal court sentenced him to 24 years in prison. He appealed his conviction to the U.S. Supreme Court. The Supreme Court heard oral arguments in March 2010. A transcript of the oral argument can be read at *http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1394.pdf*. On June 24, 2010, the U.S. Supreme Court ruled that the government had improperly applied a law used to convict Skilling. It sent the case back to a lower court. In June 2013, Skilling was sentenced to 14 years in prison. He has been in prison since 2006. His sentence will last until 2020.[13]

Why Is Accurate Financial Reporting Important?

Enron was one of many large corporate scandals in the early 2000s. These scandals shook investor confidence in the U.S. economy. The U.S. Congress held numerous hearings and committee meetings related to the aftermath of the scandal.[14] It got involved because of the scope of the fraud and the damage to Enron investors. Enron significantly misstated its financial condition in the financial statements that it filed with the SEC. Its investors lost money because of these fraudulent financial statements.

The Enron scandal showed why accurate financial information is important. Enron was able to sustain itself for at least five years due to inaccurate financial reporting. During this period, financial analysts continued to recommend its stock as a good investment. The public and Enron employees invested in it. These people had significant losses when Enron's troubles became public and the company finally declared bankruptcy. Enron duped its investors. By the time everyone knew the truth, it was too late to recover investment losses. Investors lost confidence in large public companies.

NOTE

The decade from 2000 to 2009 had some of the worst stock market performance ever.[15]

The financial statements that a company files with the SEC are one of the main sources of information that investors use to research that company. These documents help investors determine the true financial condition of a company. After the Enron scandal, the SEC required more information to be reported on these forms. It also required that the accuracy of these forms be certified in a number of different ways.

Public companies are required to file a number of financial disclosure statements with the SEC. These forms help investors understand the financial stability of a company. The most commonly filed forms are:

- **Form 10-K**—Annual report
- **Form 10-Q**—Quarterly report
- **Form 8-K**—Current report

A company uses **Form 10-K** to file its annual report. Federal law requires that publicly traded companies submit these reports each year. Depending on their size, companies must file this report within 60 to 90 days after the end of their fiscal year. The larger a company is, the faster it has to file its report.

Form 10-K is a very detailed disclosure of a company's financial condition. A company must fully describe its business in its 10-K disclosure. It must explain how it's organized and how it operates. It must provide its financial statements. These statements include balance sheets, statements of income and cash flows, and statements of shareholder equity. An independent auditor must audit the company's financial statements. The auditor's report also must be included in the Form 10-K filing.

The CEO and CFO of a company must sign the company's Form 10-K. A majority of the company's board of directors also must sign the form. The SEC estimates that it will take a company 1,998.78 hours to prepare its annual 10-K filing.[16]

Form 10-Q is a company's quarterly report. Federal law requires companies to file these reports. They must file these reports after the end of each of their first three quarters in a fiscal year. These reports are usually less detailed than the end-of-the year 10-K filing. Depending on their size, companies must file this report within 40 to 45 days after the end of each fiscal quarter.

Companies must file **Form 8-K** if they experience a major event that could affect their financial condition. Shareholders and investors should know about these events. Companies must file a Form 8-K with the SEC within four days of a major event.[17] This period is shortened in some instances. For example, a company must file Form 8-K with the SEC immediately if it becomes aware of insider trading activities.

FYI

A company's two main financial documents are its *balance sheet* and *profit and loss* statements. The balance sheet provides a summary of the company's financial condition at a certain period. They're commonly prepared on a monthly basis. A profit and loss statement is used to determine whether a company made a profit during a certain period.

General events that trigger a Form 8-K disclosure requirement include:

- Filing for bankruptcy
- Selling off significant assets
- Acquiring another company
- Getting a loan
- Board member resignation
- Board member elections
- Any changes to board governance documents

Accurate information is the "investor's best tool."[18] People need accurate financial information so that they can invest wisely and make money. The SEC recommends that potential investors carefully review a company's prospectus and financial reports. You can read the SEC's list of information that investors should review before investing at *http://www.investor.gov*. The benefit of reviewing information from a number of different sources is that an investor can get a better picture of a company's financial condition.

NOTE

A company uses a *prospectus* to describe the securities that it offers for sale. The prospectus describes the company's business plan.

It can be very hard for investors to detect fraud. This was the case in the Enron scandal. As a result, the SEC recommends that investors look for potential red flags as they review a company's financial condition. Red flags include companies that have high-value assets, but low revenues. It also includes odd items listed in the footnotes of the company's financial statements. Both of these red flags were present in the Enron scandal.

The Sarbanes-Oxley Act of 2002

Congress passed the Public Company Accounting Reform and Investor Protection Act in 2002.[19] It's more commonly known as the Sarbanes-Oxley Act of 2002. It's called SOX or Sarbox in many resources. The Act was named after its sponsors, Senator Paul Sarbanes of Maryland and Representative Michael Oxley of Ohio. It was passed in response to corporate scandals like Enron, WorldCom, and Adelphia. SOX proposed extensive changes to the Securities Act of 1933 and the Securities Exchange Act of 1934.

SOX moved through both the U.S. House of Representatives and Senate at a quick pace. It was originally introduced in the U.S. House of Representatives in February 2002. This was just months after the Enron scandal became public. On July 25, 2002, both the House and Senate voted on the final version of SOX. President George W. Bush signed SOX into law on July 30, 2002. As he signed it, he called SOX "the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt."[20]

Purpose and Scope

Congress hoped that SOX reforms would prevent another Enron scandal. The main goal of SOX is to protect shareholders and investors from financial fraud. SOX increased corporate disclosure requirements. It also created strict penalties for violations of its provisions.

SOX has 11 different titles. They are:

- **Public Company Accounting Oversight Board (Title I)**—Establishes the Public Company Accounting Oversight Board (PCAOB). The PCAOB oversees the firms that audit public companies.
- **Auditor Independence (Title II)**—Forbids auditors from providing some types of non-audit services to their clients.
- **Corporate Responsibility (Title III)**—Requires corporations to create audit committees on their board of directors. The audit committee is responsible for hiring the corporation's outside auditors.
- **Enhanced Financial Disclosures (Title IV)**—Enhances the amount of information that public companies must provide on their SEC filings. This section requires companies to report on internal controls that affect their financial reports.
- **Analyst Conflicts of Interest (Title V)**—Establishes rules to make sure that securities analysts can give independent opinions about a public company's stock risk.
- **Commission Resources and Authority (Title VI)**—Gives the SEC authority to discipline investment firms for unprofessional conduct. This section also gives the SEC additional funding to support its programs.
- **Studies and Reports (Title VII)**—Requires the SEC to review public accounting firms. The SEC must do this at least every three years. This section also requires the SEC to issue reports about how the securities market operates.
- **Corporate and Criminal Fraud Accountability (Title VIII)**—Imposes document retention requirements on companies and auditors. It protects whistleblowers. It also bans retaliation against employees who participate in fraud investigations. This section also imposes criminal penalties for violating SOX.
- **White-Collar Crime Penalty Enhancements (Title IX)**—Requires CEO and CFOs to certify that the company's financial reports fairly represent its financial condition. It creates criminal penalties for signing fraudulent statements.
- **Corporate Tax Returns (Title X)**—Is a statement from Congress that strongly suggests that a CEO sign the federal income tax return of a corporation.
- **Corporate Fraud and Accountability (Title XI)**—Establishes criminal liability for certain types of fraud committed by corporate officers. It also increases penalties for some types of corporate crime.

SOX supplements current federal securities laws. It applies to publicly traded companies that must register with the SEC. This includes international companies who trade stock on U.S. stock exchanges. SOX doesn't apply to privately held companies.

> **NOTE**
> A small public company is a company with less than $75 million of public stock.

Large public companies had to comply with all portions of SOX beginning in 2004. The SEC extended the deadline for smaller public companies several times for some of the more complicated portions of the law. It extended the deadline for the company's report on internal controls that is required by Title IV. All compliance extensions have now expired. All public companies must comply with all SOX provisions.

Main Requirements

SOX is a very detailed act. It has many provisions. This chapter focuses on the parts of the act that have had the most impact on information technology (IT) functions. When SOX was first enacted, many companies assumed that it didn't have any IT components. Congress didn't mention IT anywhere within the act.

This opinion changed as companies began to review their SOX compliance requirements. Many SOX provisions require companies to verify the accuracy of their financial information. Since IT systems hold many types of financial information, companies and auditors quickly realized that these systems were in scope for SOX compliance. That meant that how those systems are used and the controls used to safeguard those systems had to be reviewed.

The relationship between IT and SOX compliance continues to evolve. This section reviews the SOX provisions that have an IT impact. First, this section reviews the PCAOB. The PCAOB creates standards that auditors must follow when reviewing the activities of public companies. These standards help auditors determine the IT controls that they must review. The creation of the PCAOB is one of the most notable SOX reforms.

Second, this section reviews SOX provisions that impact records management functions. These provisions have an impact on IT operations because of the vast amount of data that is stored electronically. These provisions are important because they affect how IT systems are configured.

Finally, SOX requires the executive management of a company to certify that there are controls in place to protect the accuracy of company information. This is the area where SOX compliance has caused the biggest challenge for companies and IT professionals.

Public Company Accounting Oversight Board

Prior to the creation of SOX, auditors and accountants belonged to a self-regulating profession. A profession is self-regulating when it creates and enforces its own rules of conduct. Federal and state laws place few oversight requirements on members of self-regulating professions.

An attorney is a common example of a member of a self-regulating profession. Attorneys must meet minimum state law requirements to become licensed. After that, their professional behavior is largely judged by commissions made up of other attorneys who enforce rules of professional conduct. The profession itself determines what these rules of professional conduct should be.

> **FYI**
> Information security professionals belong to a largely self-regulating profession. This is especially true when information security professionals obtain certifications that require the certificate holders to follow a code of conduct.

The Enron scandal proved that self-regulation does have some drawbacks. Enron's accounting firm, Arthur Andersen, provided it with accounting, auditing, and consulting services. Enron was a large Andersen client. It paid Andersen $52 million for auditing and consulting services in 2001.[21] Even the Powers Report noted that there was a lack of critical advice from its auditors at Arthur Andersen in reviewing Enron's publicly filed financial statements.[22] This may have been because Arthur Andersen was reluctant to challenge such an important client.

Congress created the PCAOB to provide a layer of government oversight on auditing activities. The PCAOB oversees auditors that audit public companies. It was created in order to ensure that audit reports for public companies are fair and independent. Under SOX, the PCAOB has several duties.[23] It must:

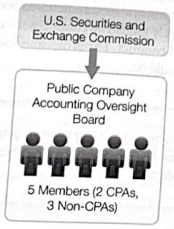
- Register accounting firms that prepare audit reports for public companies.
- Establish standards for the preparation of audit reports.
- Conduct inspections of registered public accounting firms.
- Conduct investigations and disciplinary proceedings against registered public accounting firms.
- Perform other duties or functions necessary to carry out SOX.
- Enforce SOX compliance.
- Set a budget for the PCAOB, and manage its operations.

NOTE

You can learn more about the role of the PCAOB by visiting its Web page at *http://pcaobus.org*.

The PCAOB has five members. The SEC selects these members and appoints them to staggered terms. The SEC can remove PCAOB members if needed. PCAOB members are to be "individuals of integrity and reputation who have a demonstrated commitment to the interests of investors and the public."[24] They must be financially literate. This means that they must be able to understand financial statements. Only two members of the PCAOB are allowed to be certified public accountants (CPAs). The remaining three members can't be CPAs. Members of the PCAOB aren't allowed to have any financial interest in an accounting firm. Figure 7-1 shows the structure of the PCAOB.

FIGURE 7-1
PCAOB structure.



FYI

The SEC believes that a single set of globally accepted accounting principles will benefit U.S. companies. It's evaluating whether it should adopt the International Financial Reporting Standards (IFRS). The International Accounting Standards Board has created the IFRS. You can learn about IFRS at *http://www.ifrs.com/ifrs_faqs.html*. The SEC has studied the IFRS extensively and compared them to U.S. accounting principles. As of this writing, the SEC had not yet approved IFRS for use by U.S. public companies.[25]

One of the main functions of the PCAOB is to set standards for how auditors review public companies. It has created standards related to auditing, ethics, independence, and quality control. The SEC must approve its standards. The PCAOB bases many of its standards on GAAP. The Financial Accounting Standards Board (FASB) establishes these principles. The SEC has recognized GAAP as authoritative and requires financial statements to be prepared in accordance with GAAP.

The PCAOB's Auditing Standard No. 5 provides guidance on how an auditor performs an audit of a company's internal controls over financial reporting. Auditing Standard No. 5 wasn't the PCAOB's first guidance on internal controls. Its first standard was Auditing Standard No. 2. Auditors followed this standard for the first wave of audits under SOX. Companies complained that the standard was too broad. Following it led to greater than expected costs. An Ernst & Young survey found that 85 percent of companies with revenues greater than $20 billion spent more than $10 million for SOX compliance in the first year.[26]

The PCAOB created Auditing Standard No. 5 to respond to criticisms about Auditing Standard No. 2.[27] Auditing Standard No. 5 is important for audits of IT systems and processes that impact a company's financial reports. It's important because it specifies a top-down approach that might limit the scope of review of IT systems. Auditing Standard No. 5 also recommends that auditors focus their review on areas of the highest risk.

Document Retention

SOX contains some records retention provisions. It's important to know about them because companies store many of their records electronically. Some studies estimate that 93 percent of all business documents are created and stored electronically.[28] Companies must understand how their IT systems work in order to meet SOX retention requirements.

SOX requires auditors and public companies to maintain audit papers for seven years.[29] Audit papers are most documents used in an audit. They're the materials that support the conclusions made in an audit report. SOX takes a very broad view of the type of records that must be saved. This includes work papers, memoranda, and correspondence. It also includes any other records created, sent, or received in connection with the audit. SOX also [illegible] electronic records.

Is the PCAOB Constitutional?

The constitutionality of SOX was challenged soon after it was enacted into law. The case is called *Free Enterprise Fund and Beckstead and Watts v. Public Company Accounting Oversight Board.*

The Free Enterprise Fund and Beckstead & Watts LLP filed the case in 2006. The Free Enterprise Fund is a public interest organization. Beckstead & Watts LLP is an accounting firm. The plaintiffs argued that SOX is unconstitutional. In particular, they argued that the PCAOB is unconstitutional because its creation and operation violates the constitutional separation of powers doctrine.

The plaintiffs argued that separation of powers is violated because the PCAOB is an executive branch agency that the president has virtually no control over. Under SOX, the SEC alone has the power to appoint PCAOB members. PCAOB members can be fired only for cause. Only the SEC can fire them. The president, and even the SEC, has little authority to control PCAOB members once they are appointed.

The plaintiffs argued that it violates the section of the Constitution that gives the president the power to appoint and remove officers of the executive branch. They also argued that under the Constitution, Congress isn't permitted to set up a structure that bypasses the president's authority.

The case was filed in the U.S. District Court for the District of Columbia. The District Court granted summary judgment for the PCAOB and upheld the constitutionality of SOX. In August 2008, the Circuit Court for the D.C. Court affirmed the decision of the lower court. The U.S. Supreme Court heard arguments in the case on December 7, 2009, and issued its decision in June 2010.

In its decision, the Court found that the way that the PCAOB is created does indeed violate the separation of powers doctrine. Even though the portion of SOX that creates the PCAOB is unconstitutional, however, the Court said that SOX is still good law. It also said that the PCAOB could continue to function. The Court's decision means that the SEC can now fire PCAOB members at will (or for any reason at all), instead of just for good cause.

You can view the Supreme Court's docket on the *Free Enterprise* case at *http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/08-861.htm*.

In 2010 the Dodd-Frank Wall Street Reform and Consumer Protection Act expanded the role of the PCAOB. The Act gave the PCAOB additional oversight of the audits of brokers and dealers. It gave the PCAOB the power to conduct inspections, bring enforcement action, and set standards.[30]

SOX also requires that a public company retain the records and documentation that it uses to assess its internal controls over financial reporting.[31] These controls are discussed in the next section. Guidance issued by the SEC recognizes that this documentation takes a number of different forms. It also includes electronic data. Companies must permanently retain this information.

FYI

Many federal and state laws contain records retention requirements. SOX is another law to add to that list. Organizations should develop document retention policies to help them track their different obligations.

The penalties for failing to retain records for the right amount of time can be severe. SOX makes it a crime for a person or company to knowingly and willfully violate its records retention provisions. A person who violates this provision can face fines and up to 10 years in prison.

SOX also makes it a crime for any person to tamper with or destroy any record in an attempt to interfere with a federal investigation.[32] This section was created to respond to Arthur Andersen's involvement in the Enron scandal. As soon as Enron's financial difficulties became public, partners at Arthur Andersen instructed employees to follow its document destruction policies. The company shredded thousands of Enron documents. The government later charged the company with obstructing justice. It alleged that Arthur Andersen shredded Enron documents even after it was aware that the SEC would investigate Enron. In 2005, the U.S. Supreme Court overturned Arthur Andersen's obstruction of justice conviction.

Unlike other parts of SOX, this provision applies to any organization. Private companies also must follow it. People who violate this section can face fines of up to $10 million. They also face up to 20 years in prison.

A former Ernst & Young accountant was one of the first people to be charged with violating this provision. In that case, the government alleged that the accountant altered and destroyed client audit records during a federal investigation. The Office of the Comptroller of the Currency was investigating the accountant's client at the time that he altered the documents. In October 2004, the accountant pleaded guilty. In January 2005, a federal judge sentenced him to 12 months in prison. He also received a $5,000 fine.

Companies must make sure that electronic records are stored properly so that they can satisfy SOX retention requirements. They must store the records for the right amount of time. They also must make sure that those records are destroyed properly when the retention period expires.

Certification

SOX requires companies to report accurate financial data. They must do this to protect their investors from harm. To encourage a company to report accurate data, SOX requires its CEO and CFO to certify the company's SEC filings. SOX certification provisions require executives to establish, maintain, and review certain types of internal controls for their company.

Disclosure Controls. SOX Section 302 requires CEOs and CFOs to certify a company's SEC reports. The purpose of the certifications is to put executive management on notice of the company's financial condition. The SEC can hold a CEO or CFO liable for submitting

inaccurate financial reports. It makes sense that both the CEO and CFO would have to make these certifications. They're the officers who are most knowledgeable about the company's finances and overall condition.

A certification attests to the truth of certain facts. The SEC requires a certification to be included on a number of different forms. It must be included on a company's Form 10-Q and Form 10-K reports. (These certifications don't need to be included on Form 8-K.) Under the law,[33] a CEO and CFO each must certify that:

- They have reviewed the report.
- The report doesn't contain untrue or misleading statements about the company.
- The financial statements fairly represent the company's financial condition.
- The executive is responsible for creating disclosure controls and procedures that are designed to bring material information about the company to the executive's attention, and the controls are reviewed 90 days prior to filing the report.
- The executive has disclosed all significant deficiencies in its internal controls to their auditor.
- Whether any significant changes in the internal controls have occurred since they were last evaluated.

The controls required under Section 302 are called **disclosure controls.** They are very broad. They're the processes and procedures that a company puts in place to make sure that it makes timely disclosures to the SEC. They're how management stays informed about the company's operations. These controls must address any change in information that affects company resources. They bring events to the executive's attention so that they can be reported to the SEC.

Disclosure controls are different from SOX **internal controls.** Internal controls are the processes and procedures that a company uses to provide reasonable assurance that its financial reports are reliable. The next section reviews these controls. Internal controls address only processes that protect the reliability of financial reports. Disclosure controls are broader. They include internal controls.[34] Figure 7-2 shows the relationship between disclosure controls and internal controls.

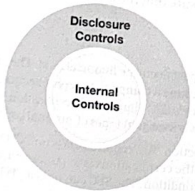


FIGURE 7-2
Relationship between disclosure controls and internal controls.

SOX Section 906 imposes criminal liability for fraudulent certifications. Under this section, CEOs and CFOs that knowingly certify fraudulent reports may be fined up to $1 million. They also could be imprisoned for up to 10 years. An officer who willfully makes a fraudulent certification may be fined up to $5 million. They could be imprisoned up to 20 years.

> **NOTE**
> SOX sections 302 and 906 were created in response to the Enron scandal. Would Enron's executives have acted differently if they had been required to make these certifications on SEC filings?

Internal Controls. SOX Section 404 requires a company's executive management to report on the effectiveness of the company's internal controls over financial reporting (ICFR). They must make this report each year on their Form 10-K filing. Under this section, management must create, document, and test ICFR. After management makes its yearly report on its ICFR, outside auditors must review the report and verify that the ICFR work. This section has caused compliance headaches for IT professionals.

Under SEC rules, ICFR are processes that provide reasonable assurance that financial reports are reliable.[35] ICFR provide management with reasonable assurance that:

- Financial reports, records, and data are accurately maintained
- Transactions are prepared according to GAAP rules and are properly recorded
- Unauthorized acquisition or use of data or assets that could affect financial statements will be prevented or detected in a timely manner

SOX doesn't define reasonable assurance. The SEC and PCAOB recognize that reasonable assurance doesn't mean absolute assurance.[36] However, it's a high level of assurance that satisfies management that ICFR are effective. Management must be confident that these controls protect financial reporting mechanisms.

The SEC requires that management use evaluation criteria established by recognized experts to review the company's ICFR. The evaluation criteria helps to ensure that ICFR are effective. The SEC has recognized only one specific framework that meets its requirements: the COSO Framework. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission first created its "Internal Control—Integrated Framework" in 1992. It revised this framework in 2013. The framework is commonly called the "COSO Framework." Many U.S. businesses use this framework to assess their internal control systems.[37] The 1992 version of the COSO Framework didn't directly address IT or information security goals. The 2013 version of the Framework recognized that it's also necessary to implement control activities over technology implementations.[38]

Companies trying to comply with Section 404 quickly learned that they needed to review their IT systems. Specifically, they needed to review the ICFR on their IT systems. An Ernst & Young survey found that public companies spent 70 percent of their time addressing IT controls in their first year of SOX compliance.[39] Companies spent a lot of time on IT controls because information systems contain financial data. An error in these systems could cause financial statements to contain errors or mistakes. To comply with Section 404, companies had to make sure that system data was accurate. They had to make sure that they had processes in place to detect inaccurate data.

What Is COSO?

COSO was established in 1985 to identify factors that contributed to fraudulent financial reporting. Five U.S. financial organizations sponsored COSO. They are the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants. COSO is a nonprofit organization.

In 1987, COSO issued a report on the factors that contribute to fraudulent financial reporting. Its report contained 49 recommendations to prevent and detect fraudulent financial reports. You can read the 1987 report at *https://www.coso.org/Documents/NCFFR.pdf*. Many SOX provisions mirror the report's recommendations. One of these recommendations called for the creation of effective ICFR.

In 1992, COSO issued guidance on internal controls. The COSO framework says that internal controls are effective when they give the management of a company reasonable assurance that:

- It understands how the entity's operational objectives are being achieved
- Its published financial statements are being prepared reliably
- It's complying with applicable laws and regulations

The COSO Framework was updated in 2013. It was updated because the business environment has grown more complex since the framework was initially issued. COSO estimates that it will take organizations some time to review and adopt the new framework. It has proposed a number of transition approaches. It anticipates that companies will transition to the new framework through the end of 2014.[40]

The COSO Framework has five components. They are:

- **Control environment**—This is the organization's culture. Control environment factors include management philosophy and the competence of the organization's people. The control environment sets the foundation for the other components of the framework.
- **Risk assessment**—This refers to the identification and review of risks that are internal and external to the organization.
- **Control activities**—This refers to how policies and procedures are followed throughout the organization.
- **Information and communication**—This addresses how an organization communicates information internally to its employees. It also addresses how an organization communicates to external parties. This component also addresses how information systems store and generate data.
- **Monitoring**—This refers to how the organization monitors its internal control systems.

You can learn more about COSO's "Internal Control—Integrated Framework" by visiting *https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf*.

SOX Section 404 compliance isn't easy. Section 404 is very general about the types of ICFR that companies must implement. It doesn't give a good definition for ICFR generally. It doesn't address IT controls at all. In 2007, the SEC issued additional guidance to help companies assess ICFR during their Section 404 review. It did this in response to many complaints about the large scope of a Section 404 review. Many of these complaints focused on how to address IT controls.

The SEC stated two broad principles in its guidance:

- Management should assess how its internal controls prevent or detect significant deficiencies in financial statements
- Management should perform a risk-based review of the effectiveness of these controls

> **NOTE**
> SOX doesn't specify the IT controls that companies need to implement. Instead, companies must determine the best controls for their own systems.

The SEC also said that management must exercise its professional judgment to limit the scope of a Section 404 review. It reminded companies that SOX applies to internal controls, including IT controls, that affect financial reporting only.[41]

Management must review general IT controls to make sure that IT systems operate properly and consistently. The controls must provide management with reasonable assurance that IT systems operate properly to protect financial reporting. Table 7-1 shows how the goals of ICFR match up with information security goals.

It's clear that management's review of an organization's ICFR must include a review of IT controls as well. The COSO Framework doesn't specifically address the types of IT controls that an organization should implement. Organizations use many approaches to evaluating their IT controls. Some organizations follow the Guide to Assessment of IT Risk (GAIT) framework. Others use COBIT. Both of these frameworks appear to meet the SECs requirements for a suitable evaluation framework.

Some companies outsource functions, but a company can't escape SOX Section 404 liability by outsourcing financial functions. SOX requires companies to monitor ICFR for outsourced operations as well. Many companies do this by asking their outsourcing companies to provide them with a Service Organization Control (SOC) report.

TABLE 7-1 Internal controls and information security goals.

STEPS TAKEN TO MEET INTERNAL CONTROLS	INFORMATION SECURITY GOALS
Financial reports, records, and data are accurately maintained.	Integrity
Transactions are prepared according to GAAP rules and properly recorded.	Integrity, availability
Unauthorized acquisition or use of data or assets that could affect financial statements will be prevented or detected in a timely manner.	Confidentiality, integrity, availability

The American Institute of Certified Public Accountants (AICPA) created the Statement on Standards for Attestation Engagements 16, "Reporting on Controls at a Service Organization." Reports created under this standard are known as SOC reports. An SOC report is a report on a service organization. Service organizations are organizations that provide services to others.

SOC audits review the service organization's control activities related to the services that it provides to its customers. These audits review the IT controls on the outsourced service. A SOC audit helps a service organization show that they have proper safeguards in place to protect their customer's data.

There are three levels of SOC reports:

- **SOC 1**—Report on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting. These reports are used by auditors to assess the ICFR at one entity that does business with another entity. These reports are generally only shared between the organizations that are doing business with one another.
- **SOC 2**—Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy. These reports are used by an entity to demonstrate that it has good information security practices to potential customers. These reports specifically address security, availability, processing integrity, confidentiality, and privacy. These reports may be shared with potential customers. They are usually shared under a confidentiality agreement so the information in the report is kept private.
- **SOC 3**—Trust Services Report for Service Organizations. These reports are similar to SOC 3 reports. However, they don't contain the same level of detail regarding information system operations. These reports only contain the auditor's assessment of whether or not the outsourced functions meet certain control objectives. They do not contain details about those functions. These reports may be widely shared with potential customers.[42]

Many companies may ask a service provider to share their SOC 2 or SOC 3 report. They might do this before entering into an outsourcing relationship. Many service organizations have these reports prepared in advance so that they can respond quickly to a customer request.

Oversight

The Securities and Exchange Commission oversees most SOX provisions. The SEC was created under the Securities and Exchange Act of 1934. Its mission is to protect investors and maintain the integrity of the securities industry.

The SEC has five commissioners. The U.S. President must appoint them. They serve for five-year terms. No more than three of the commissioners may belong to the same political party. The SEC has 11 regional offices in the United States.[43]

SOX gives the SEC specific duties. The SEC is required to designate the members of the PCAOB. It's also required to review various operations of public companies to make sure that they're following SOX.

SOX requires the SEC to review a public company's Form 10-K and Form 10-Q reports at least once every three years.[44] It must do this to try to detect fraud and inaccurate financial statements that could harm the investing public. The SEC has discretion in deciding how often to review companies. SOX states the factors that the SEC should consider when deciding to conduct a review. Under SOX, the SEC must consider:

- Whether a company has amended its financial reports
- Whether a company's stock price fluctuates significantly when compared to other companies
- How much stock the company has issued
- The difference between a company's stock price and its earnings
- Whether a company is large and affects a particular sector of the economy
- Any other factor that the SEC considers relevant

The SEC enforces SOX compliance. It has the power to investigate and sanction public companies that don't comply with SOX.

Compliance and Security Controls

Assessing ICFR in IT systems can be difficult. IT professionals have a number of different frameworks that they can use for reviewing IT controls. You are already familiar with some of these frameworks. Many of these frameworks help companies decide which controls to implement.

COBIT

In 1996, the Information Systems Audit and Control Association (ISACA) released the first version of "Control Objectives for Information and related Technology" (COBIT). The fifth edition of COBIT was released in 2012.[45] ISACA has moved away from use of the term "control objective" in the most recent version of COBIT. However, it kept the popular term "COBIT" for the name of its framework.

ISACA recognizes that "information is a key resource for all enterprises."[46] COBIT 5 is revolutionary. Previous versions of COBIT addressed only information technology requirements independent of the business goals of an organization. The COBIT 5 framework is much larger. Its aim is to help organizations create value from its information technology assets. COBIT provides a framework for the governance and management of those assets. It has five key principles:

The ISO/IEC standards are specific to information security. Companies can use these standards to make sure that their information security practices provide reasonable assurance that ICFR are effective. See Table 7-1 for the relationship between SOX internal controls and information security goals.

NIST Computer Security Guidance

Finally, some organizations turn to the National Institute of Standards and Technology (NIST) for information security control guidance. NIST creates information security guidance for federal agencies. These agencies must comply with the Federal Information Security Management Act (FISMA).

Many non-governmental organizations also use NIST publications to guide their own information security programs. "NIST Special Publication 800-53 (Rev. 4), Security and Privacy Controls for Federal Information Systems and Organizations" states the minimum security controls that organizations should use to create an effective information security program.

You can learn more about NIST computer security resources at *http://csrc.nist.gov/*

SOX doesn't provide public companies with specific advice on how to use IT controls. Many organizations use the frameworks reviewed in this chapter to guide their SOX Section 404 compliance activities.

SOX Influence in Other Types of Companies

With few exceptions, SOX applies only to public companies. However, many different types of organizations have been affected by SOX. This is because SOX promotes good corporate governance practices. Many of these principles make sense for other organizations as well.

In addition to the certification provisions discussed earlier, SOX governance provisions include:

- **Independent directors**—SOX requires a public company to create an independent board of directors. Directors are independent when they don't have financial ties to the company. In some cases, the independence rules extend to members of the director's immediate family.
- **Audit committee**—SOX requires public companies to have an audit committee on their board of directors. This committee works with outside auditors to make sure that financial reports are accurate.
- **Conflicts of interest**—SOX requires executives to disclose certain types of conflicts of interest

A private company might implement SOX controls because it hopes to become a public company someday. Following SOX principles will make the transition from private to public easier. If a private company follows SOX principles, it might be in a better position

to attract investors. It will have processes in place that allow investors to review the company's financial condition. Investors will be more likely to invest in companies that show financial transparency.

Nonprofit organizations also have an incentive to follow SOX. Good governance in a nonprofit organization is very important. Nonprofits depend on grants from other entities to support their operations. They also depend on individual donations. People won't contribute to nonprofits that aren't managed well. Nonprofits that adopt SOX governance principles can prove that they have controls in place to properly manage the organization and its finances. A reputation for good governance also will encourage more donations.

> **NOTE**
> A nonprofit organization doesn't distribute its profits to owners or shareholders. Instead, it puts its profits back into the organization to help pursue its goals. Many charities are nonprofit organizations.

In some ways, SOX truly has become a best practice for good governance. Companies that follow SOX practices prove that they have controls in place to prevent and detect wrongdoing. This can be important if a company is involved in litigation about bad governance practices. A plaintiff's lawyer will surely point out if a board didn't follow SOX good governance practices. It won't matter whether the company was required by law to follow SOX or not. Since SOX is a best practice that many companies follow, the implication that a company didn't follow SOX can be damaging.

Corporate Privacy Issues

Corporate information privacy covers a number of issues. Since companies have a number of different kinds of records, they must approach privacy from many angles. The three major corporate privacy concerns are:

- Privacy of employee data
- Privacy of customer data
- Privacy of corporate data

In general, employees have no expectation of privacy in their workplaces. In most cases, this means that employers can monitor an employee's work activities. It includes monitoring telephone and e-mail conversations. Employers can also monitor employee Internet access and computer use. In most cases, it's best if employers give their employees notice that they're monitoring employees in this way.

Employers also can monitor employee workspaces and offices. They can use closed circuit television (CCTV) or other video tools to do this. Like other types of monitoring, it's best if the employer gives notice about the monitoring. While the ability to monitor is broad, employers usually can't monitor locations like bathrooms, locker rooms, and employee lounges. Some courts have held that employees do have a reasonable expectation of privacy in these areas.

Companies must protect certain types of information belonging to their employees. For example, if a company provides an employee health plan, it must keep some information private. The Health Insurance Portability and Accountability Act (HIPAA) requires companies to protect some information about employee health plans. A company with an on-site health clinic must protect employee medical records under HIPAA and state laws.

Companies also must protect customer data. Some companies must protect consumer information in special ways. For example, the Gramm-Leach-Bliley Act (GLBA) requires companies to protect consumer financial information. Some states also have laws that require companies to protect the personally identifiable information (PII) of their customers. If the company suffers a security breach that compromises PII, then it must inform its customers about the breach. These laws are called data breach notification laws. The purpose of these laws is to help protect people from identity theft.

Finally, companies have their own internal records to protect. These records may contain data about the company's organization, finances, human resources, and legal matters. In general, a company's directors and officers always have the ability to see all company records. In a small company, the owner has this right. They also can enter employee offices to review records. They have the ability to do this in the regular course of business. This is because they are responsible for the business and its successful operation.

In corporations, the directors of a company have an absolute right to be able to inspect the company's records. Shareholders also have a right to inspect corporate records. However, the shareholder's inspection right is not as broad as a director's right. In most states, shareholders have a right to inspect some records during regular business hours. They must make a written request to inspect corporate records. The request must include the shareholders' reason for wanting to review the records.

Companies also have records regarding their products and services that they must protect. Some of these records might be trade secrets. Trade secrets are information about company products or services that helps one company compete against another company. Trade secrets are a form of intellectual property. A company must protect its trade secret information. If it properly protects this kind of information, it's entitled to legal protection.

Case Studies and Examples

Investors can learn about a company's financial information from many different places. One place to learn information is from the SEC's Electronic Data Gathering and Retrieval (EDGAR) database. All public companies that are required to register with the SEC file their required reports through EDGAR.

You can search for a public company's filings on EDGAR. The URL is *http://www.sec.gov/edgar/searchedgar/companysearch.html.*

Pick a public company and try to search for it on EDGAR. Good companies to search include Microsoft Corp., Apple Inc., Starbucks Corp., and the Walt Disney Company. Look at the company's most recent Form 10-K report. Item 9A is the SOX Section 404 report on internal controls. What do these sections tell you? What can you learn about the company that you have searched? You can learn more about how to read these forms at *http://www.sec.gov/answers/reada10k.htm.*

CHAPTER SUMMARY

Congress created the Sarbanes-Oxley Act in response to scandal. It passed SOX to help improve investor confidence in publicly traded companies. SOX places rules on public companies and other organizations. These rules promote trustworthy financial reports. The scope of SOX extends to any public company functions or processes that impact financial reporting. The scope of SOX within a company is very broad. SOX requires that companies review many information technology processes to make sure that they're trustworthy.

The scope of SOX is broad. Its influence extends even to organizations that aren't required to follow it. For example, private companies and nonprofit organizations may choose to follow SOX to show their commitment to good governance.

KEY CONCEPTS AND TERMS

Disclosure controls
Dividend
Form 8-K
Form 10-K
Form 10-Q
Internal controls
Privately held company
Public company
Securities