CHAPTER

15

Auditing IT Controls Part I: Sarbanes-Oxley and IT Governance

This chapter introduces the topic of IT auditing. It begins with an overview of the key components of an audit. Next, the chapter turns to internal control and audit issues related to Sections 302 and 404 of SOX. This section reviews the Management and auditor responsibilities under SOX. The section concludes with a discussion of computer fraud issues. The next section of the chapter presents risks and controls related to IT governance. The structure of the IT function within an organization and the risks that can arise from inappropriate structuring are issues of concern. The chapter then moves on to a review of computer center threats and controls, which include protecting against natural disasters, fire, temperature, and humidity. The chapter discusses important issues related to disaster recovery including provision for second-site backup, identifying critical applications, performing backup and off-site storage procedures and preparing a disaster recovery plan. The final section of the chapter examines issues surrounding the growing trend toward IT outsourcing. This popular practice is associated with both significant benefits and risks, which are addressed. The chapter concludes with a discussion of audit issues related to outsourcing including the SSAE 16 reporting standard.

Learning Objectives

After studying this chapter, you should:

- Be familiar with the structure of a financial audit and the role of the IT audit component.
- Understand the key features of Sections 302 and 404 of the Sarbanes-Oxley Act.
- Understand management and auditor responsibilities under Sections 302 and 404.
- Understand the risks of incompatible functions and how to structure the IT function.
- Be familiar with the controls and precautions required to ensure the security of an organization's computer facilities.
- Understand the key elements of a disaster recovery plan.
- Be familiar with the benefits, risks, and audit issues related to IT outsourcing.

Overview of Auditing

An external audit is an independent attestation performed by an expert—the auditor—who expresses an opinion regarding the presentation of financial statements. This attest service is performed by Certified Public Accountants (CPA) who work for public accounting firms that are independent of the client organization being audited. The audit objective is always associated with assuring the fair presentation of financial

statements. These audits are, therefore, often referred to as *financial audits.* The Securities and Exchange Commission (SEC) requires that all publicly traded companies be subject to a financial audit annually. CPAs conducting such audits represent the interests of outsiders: stockholders, creditors, government agencies, and the general public.

The CPA's role is to collect and evaluate **evidence** and thus render an opinion. A key concept in this process is *independence.* The judge must remain independent in his or her deliberations and cannot be an advocate of either party in a trial. The judge must apply the law impartially based on the evidence presented. Likewise, the independent auditor collects and evaluates evidence, and renders an opinion based on the evidence. Throughout the audit process, the auditor must maintain independence from the client organization. Public confidence in the reliability of the company's internally produced financial statements rests directly on an evaluation of them by an independent auditor.

External auditors follow strict rules in conducting financial audits. These authoritative rules have been defined by the SEC, the Financial Accounting Standards Board (FASB), the American Institute of Certified Public Accountants (AICPA), and by federal law (Sarbanes-Oxley Act of 2002). With the passage of SOX, Congress established the Public Company Accounting Oversight Board (PCAOB), which has to a great extent replaced the function served by the FASB, and some of the functions of the AICPA (e.g., setting standards and issuing reprimands and penalties for CPAs who are convicted of certain crimes or found guilty of certain infractions). Regardless, under federal law the SEC has final authority over financial auditing.

Financial Audit Components

The product of the attestation function is a formal written report that expresses an opinion as to whether the financial statements are in conformity with *generally accepted accounting principles (GAAP).* External users of financial statements are presumed to rely on the auditor's opinion about the reliability of financial statements in making decisions. To do so, users must be able to place their trust in the auditor's competence, professionalism, integrity, and independence. Auditors are guided in their professional responsibility by the 10 *generally accepted auditing standards (GAAS)* presented in Table 15-1.

TABLE 15-1 GENERALLY ACCEPTED AUDITING STANDARDS

General Standards	Standards of Field Work	Reporting Standards
1. The auditor must have adequate technical training and proficiency.	1. Audit work must be adequately planned.	1. The auditor must state in the report whether financial statements were prepared in accordance with generally accepted accounting principles.
2. The auditor must have independence of mental attitude.	2. The auditor must gain a sufficient understanding of the internal control structure.	2. The report must identify those circumstances in which generally accepted accounting principles were not applied.
3. The auditor must exercise due professional care in the performance of the audit and the preparation of the report.	3. The auditor must obtain sufficient, competent evidence.	3. The report must identify any items that do not have adequate informative disclosures.
		4. The report shall contain an expression of the auditor's opinion on the financial statements as a whole.

AUDITING STANDARDS

Auditing standards are divided into three classes: general qualification standards, field work standards, and reporting standards. Although GAAS establishes the framework for prescribing auditor performance, it is not sufficiently detailed to provide meaningful guidance in specific circumstances. To provide specific guidance, the AICPA issues *Statements on Auditing Standards (SASs)* as authoritative interpretations of GAAS.

The first SAS (SAS 1) was issued by the AICPA in 1972. Since then, many SASs have been issued to provide auditors with guidance on a spectrum of topics, including methods of investigating new clients, procedures for collecting information from attorneys regarding contingent liability claims against clients, and techniques for obtaining background information on the client's industry.

Statements on Auditing Standards are regarded as authoritative pronouncements because every member of the profession must follow their recommendations or be able to show why a SAS does not apply in a given situation. The burden of justifying departures from the SASs falls upon the individual auditor.

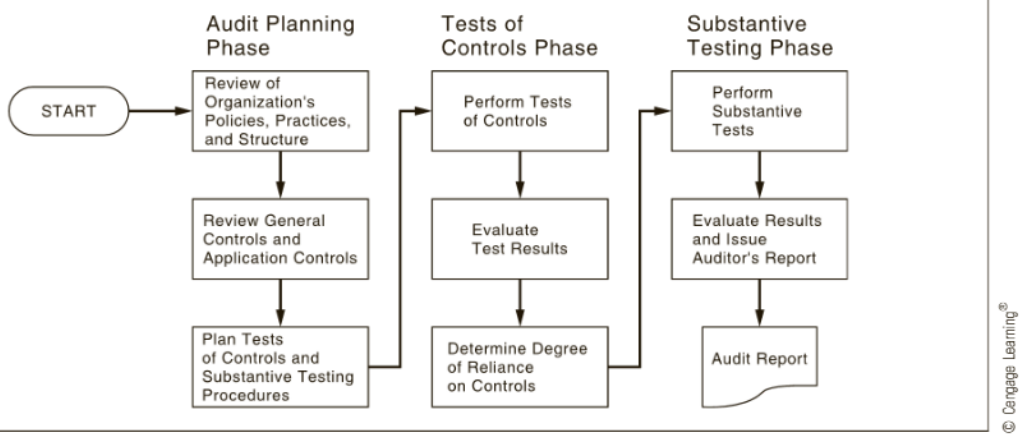
Structure of an Audit

Conducting an audit is a systematic and logical process that consists of three conceptual phases: audit planning, tests of controls, and substantive testing. Figure 15-1 illustrates the steps involved in these phases. An **IT audit** involves specialized procedures that are directed to those aspects of the client's system where technology plays a material role and thus injects an added degree of complexity into the audit. For example, transaction processing in an IT environment involves automated procedures performed by computer programs and digital source documents, journals, and ledgers that are stored in relational databases. Since modern accounting information systems employ significant levels of technology, IT auditing often constitutes a substantial component of the overall financial audit.

AUDIT PLANNING

The first phase of the audit is **audit planning**. Before the auditor can determine the nature and extent of the tests to be performed, he or she must gain a thorough understanding of the client's business. The auditor's objective at this point is to obtain sufficient information about the firm to

FIGURE 15-1 PHASES OF AN AUDIT



plan the other phases of the audit. During this phase the auditor attempts to understand the organization's policies, practices, and structure. The auditor also identifies the financially significant applications and attempts to identify and understand the controls over the transactions that are processed by these applications.

The techniques for gathering evidence at this phase include administering questionnaires, interviewing management, reviewing systems documentation, and observing day-to-day activities. The audit then proceeds to the next phase, where the auditor tests the controls for compliance with preestablished standards.

Tests of Controls

The objective of the **tests of controls** phase is to determine whether adequate internal controls are in place and functioning properly. The evidence-gathering techniques used in this phase include both manual techniques and specialized computer audit techniques known as **computer-aided audit tools and techniques (CAATTs)**. These techniques are discussed in detail in Chapter 17. At the conclusion of the tests-of-controls phase, the auditor assesses the quality of the internal controls by assigning a level for **control risk**. The level of risk ascribed to internal controls will affect the nature and extent of substantive testing that needs to be performed in the third phase. Control risk is discussed later in this section.

Substantive Testing

The third phase of the audit process focuses on gathering evidence pertaining to financial data. This phase involves a detailed investigation of specific account balances and transactions through what are called **substantive tests**. For example, a customer confirmation is a substantive test used to verify account receivable balances. The auditor selects a sample of customer accounts and contacts these customers directly to determine if the amount stated in the AR is correct and is owed by a bona fide customer. By so doing, the auditor determines the accuracy of sample and draws a conclusion about the fair value of the entire accounts receivable account as presented in the financial statements.

Substantive tests tend to be physical, labor-intensive activities such as counting cash, counting inventories in a warehouse, and verifying the existence of stock certificates in a safe. Much of the data needed to perform substantive tests (such as account balances and customer names and addresses) are stored in digital form in data files and must be extracted using CAATTs software.[1] The nature (what to examine), timing (when to examine), and extent (how many items to examine) of substantive tests are audit decisions that are driven by the concepts of management assertions and audit risk. These topics are discussed in the following sections.

MANAGEMENT ASSERTIONS

Management assertions are claims made by management regarding the content of their issued financial statements. Implicitly management asserts that account balances and underlying transactions are free from material errors and are complete, valid, and accurate. Through substantive procedures auditors gather evidence to test the validity of management assertions, which fall into the general categories below:[2]

1. Assertions about classes of transactions and events for the period under audit:
   - Occurrence. Transactions and events that have been recorded have occurred and pertain to the entity.
   - Completeness. All transactions and events that should have been recorded have been recorded.
   - Accuracy. Amounts and other data relating to recorded transactions and events have been recorded appropriately.

1 Chapter 17 describes the use of CAATTs in performing substantive tests.

2 Source: SAS No. 106.

- Cutoff. Transactions and events have been recorded in the correct accounting period.
- Classification. Transactions and events have been recorded in the proper accounts.

2. Assertions about account balances at the period end:
   - Existence. Assets, liabilities, and equity interests exist.
   - Rights and obligations. The entity holds or controls the rights to assets, and liabilities are the obligations of the entity.
   - Completeness. All assets, liabilities, and equity interests that should have been recorded have been recorded.
   - Valuation and allocation. Assets, liabilities, and equity interests are included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments are appropriately recorded.
3. Assertions about presentation and disclosure:
   - Occurrence and rights and obligations. Disclosed events and transactions have occurred and pertain to the entity.
   - Completeness. All disclosures that should have been included in the financial statements have been included.
   - Classification and understandability. Financial information is appropriately presented and described and disclosures are clearly expressed.
   - Accuracy and valuation. Financial and other information are disclosed fairly and at appropriate amounts.

The auditors develop **audit objectives** and design **audit procedures** to gather evidence that corroborates or refutes management's assertions. Table 15-2 provides some examples to illustrate the relationship between management assertions, audit objectives, and audit procedures.

TABLE 15-2 AUDIT OBJECTIVES AND AUDIT PROCEDURES BASED ON MANAGEMENT ASSERTIONS

Management Assertion	Audit Objective	Audit Procedure
Existence	Inventories listed on the balance sheet exist.	Observe the counting of physical inventory.
Completeness	Accounts payable include all obligations to vendors for the period.	Compare receiving reports, supplier invoices, purchase orders, and journal entries for the period and the beginning of the next period.
Rights and Obligations	Plant and equipment listed in the balance sheet are owned by the entity.	Review purchase agreements, insurance policies, and related documents.
Valuation or Allocation	Accounts receivable are stated at net realizable value.	Review entity's aging of accounts and evaluate the adequacy of the allowance for uncorrectable accounts.
Classification and Understandability	Contingencies not reported in financial accounts are properly disclosed in footnotes.	Obtain information from entity lawyers about the status of litigation and estimates of potential loss.

AUDIT RISK

Audit risk is the probability that the auditor will render an unqualified (clean) opinion on financial statements that are, in fact, materially misstated because of undetected errors or irregularities or both. Errors are unintentional mistakes. Irregularities are intentional misrepresentations associated

with the commission of a fraud, such as misappropriation of physical assets or attempts to deceive financial statement users.

Audit Risk Components

The auditor's objective is to achieve a level of audit risk that is acceptable to the auditor. The auditor estimates acceptable audit risk (AR) based on the *ex ante* value of the components of the audit risk model—inherent risk, control risk, and detection risk.

Inherent Risk

Inherent risk (IR) is associated with the unique characteristics of the business or industry of the client.[3] Firms in declining industries have greater inherent risk than firms in stable or thriving industries. Likewise, industries that have a heavy volume of cash transactions have a higher level of inherent risk than those that do not. Furthermore, valuating inventory when the type of inventory is difficult to value due to its nature is associated with higher inherent risk than in situations where inventory values are more objective. For example, the valuation of diamonds is inherently more risky than assessing the value of automobile tires. Auditors cannot reduce the level of inherent risk. Even in a system protected by excellent controls, financial data and, consequently, financial statements can be materially misstated.

Control Risk

Control risk (CR) is the likelihood that the control structure is flawed because controls are either absent or inadequate to prevent or detect errors in the accounts.[4] To illustrate control risk, consider the following partial customer sales record, which is processed by the sales order system.

Quantity	Unit Price	Total
10 Units	$20	$2,000

Assuming the Quantity and Unit Price fields in the record are correctly presented, the extended amount (Total) value of $2,000 is in error. An accounting information system (AIS) with adequate controls should prevent or detect such an error. If, however, controls are lacking, and the value of Total in each record is not validated before processing, then the risk of undetected errors entering the data files increases.

Auditors assess the level of control risk by performing tests of internal controls. In the preceding example, the auditor could create test transactions, including some with incorrect Total values, which are processed by the application in a test run. The results of the test will indicate that price extension errors are not detected and are being incorrectly posted to the accounts receivable file.

Detection Risk

Detection risk (DR) is the risk that auditors are willing to take that errors not detected or prevented by the control structure will also go undetected by the auditor as he or she performs substantive tests. Auditors predetermine an acceptable level of detection risk (called planned detection risk), which influences the level of substantive tests that they must perform. For example, a planned detection risk of 10 percent requires more substantive testing that a detection is set at 20 percent. As we shall see next, the more reliable the internal controls, the more planned detection risk the auditor can assume, and less substantive testing is required.

3 Auditing Standards Board, *AICPA Professional Standards* (New York: AICPA, 1994), AU Sec. 312.20

4 Ibid.

Audit Risk Model

Auditors use the audit risk components in the model below to determine the scope, nature, and timing of substantive tests.

$$AR = IR \times CR \times DR$$

Assume that acceptable audit risk is assessed at a value of 5 percent, consistent with the 95 percent confidence interval associated with statistics. Further assume that IR is assessed at 40 percent, and CR is assessed at 60 percent. What level of planned detection risk (DR) is needed to achieve the acceptable audit risk (AR) of 5%?

$$5\% = 40\% \times 60\% \times DR$$
$$DR = .05/.24$$
$$DR = .20$$

Let's now reduce the control risk (CR) value to 40% and recalculate DR.

$$5\% = 40\% \times 40\% \times DR$$
$$DR = .31$$

Notice that to achieve an acceptable level of audit risk in the first example, the auditor must set planned detection risk lower (20%) than in the second example (31%). This is because the internal control structure in the first example is more risky (60%) than it is in the second case (40%). This greater risk necessitates more substantive testing to ensure that no material errors go undetected by the auditor.

In summary, the stronger the internal control structure, as determined through tests of controls, the lower the control risk, and the less substantive testing the auditor must do. This relationship is true because the likelihood of errors in the accounting records is reduced when controls are strong. Therefore, when controls are in place and effective, the auditor may limit substantive testing. In contrast, the weaker the internal control structure, the greater the control risk, and the more substantive testing the auditor must perform to reduce total audit risk. Evidence of weak controls thus forces the auditor to extend substantive testing to search for misstatements.

Audit Report

Upon completion of the audit the auditor submits an **audit report** to the audit committee of the board of directors. The audit report includes an opinion on the fair presentation of the financial statements and an opinion on the quality of internal controls over financial reporting. A single material weakness in the internal controls requires the auditor to issue a qualified opinion regarding internal controls over financial reporting. This does not mean, however, that the auditor's opinion on the financial statements must also be qualified. If the auditor can conclude through additional tests that the internal control weakness did not result in material misstatement of the financials, the auditor may issue an unqualified (clean) opinion on the financial statements while simultaneously issuing a qualified opinion on the internal controls.

Overview of SOX Sections 302 and 404

SOX of 2002 established corporate governance regulations and standards for public companies registered with the Securities and Exchange Commission (SEC). Although the act contains many sections, this chapter and the two following chapters concentrate on internal control and audit responsibilities pursuant to Sections 302 and 404.

Section 302 requires corporate management, including the chief executive officer (CEO), to certify financial and other information contained in the organization's quarterly and annual reports. The rule also requires corporate management to certify the internal controls over financial reporting. The certifying officers are required to have designed internal controls, or to have caused such controls to be designed, and to provide reasonable assurance as to the reliability of the financial

reporting process. Furthermore, they must disclose any material changes in the company's internal controls that have occurred during the most recent fiscal quarter.

Section 404 requires the management of public companies to assess the effectiveness of their organization's internal controls over financial reporting. Under this section of the act, management is required to provide an annual report addressing the following points:

1. Describe the flow of transactions, including IT aspects, in sufficient detail to identify points at which a misstatement could arise.
2. Using a risk-based approach, assess both the design and operating effectiveness of selected internal controls related to material accounts.[5]
3. Assess the potential for fraud in the system and evaluate the controls designed to prevent or detect fraud.
4. Evaluate and conclude on the adequacy of controls over the financial statement reporting process.
5. Evaluate entity-wide (general) controls that correspond to COSO internal control framework.

Regarding the final point, the SEC has made specific reference to COSO as a recommended control framework. Furthermore, the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5 endorses the use of COSO as the framework for control assessment. Although other suitable frameworks have been published, any framework used should encompass all of COSO's general themes.[6]

RELATIONSHIP BETWEEN IT CONTROLS AND FINANCIAL REPORTING

Information technology drives the financial reporting processes of modern organizations. Automated systems initiate, authorize, record, and report the effects of financial transactions. As such, they are inextricable elements of the financial reporting processes that SOX considers, and must be controlled. The COSO model identifies two broad groupings of IT controls: application controls and general controls. As we saw in previous chapters, **application controls** ensure the validity, completeness, and accuracy of financial transactions. These controls are designed to be application-specific. Examples include:

- A cash disbursements batch balancing routine that verifies that the total payments to vendors reconciles with the total postings to the accounts payable subsidiary ledger.
- An accounts receivable check digit procedure that validates customer account numbers on sales transactions.
- A payroll system limit check that identifies employee time card records with reported hours worked in excess of the predetermined normal limit.

These examples illustrate how application controls have a direct impact on the integrity of data that make their way through various transaction processing systems and into the financial reporting process. IT **general controls** are so named because they are not application-specific, but rather apply to all systems. General controls have other names in other frameworks, including **general computer controls** and **information technology controls**. Whatever name is used, they include controls over IT governance, IT infrastructure, network and operating system security, databases access, application acquisition and development, and program changes.

Although general controls do not control specific transactions, they have an effect on transaction integrity. For example, consider an organization with poor database security controls. In such a situation, even data processed by systems with adequate built-in application controls may be at risk from an individual who circumvents database security (either directly or via a malicious

5 Management should design their assessment based on risks specific to the organization rather than follow a one-size-fits-all checklist.

6 A popular competing control framework is Control Objectives for Information and Related Technology (COBIT), published by the IT Governance Institute (ITGI). This framework maps into COSO's general themes.

program) and changes, steals, or corrupts stored transaction data. Thus, general controls are needed to support the environment in which application controls function, and both are needed to ensure accurate financial reporting.

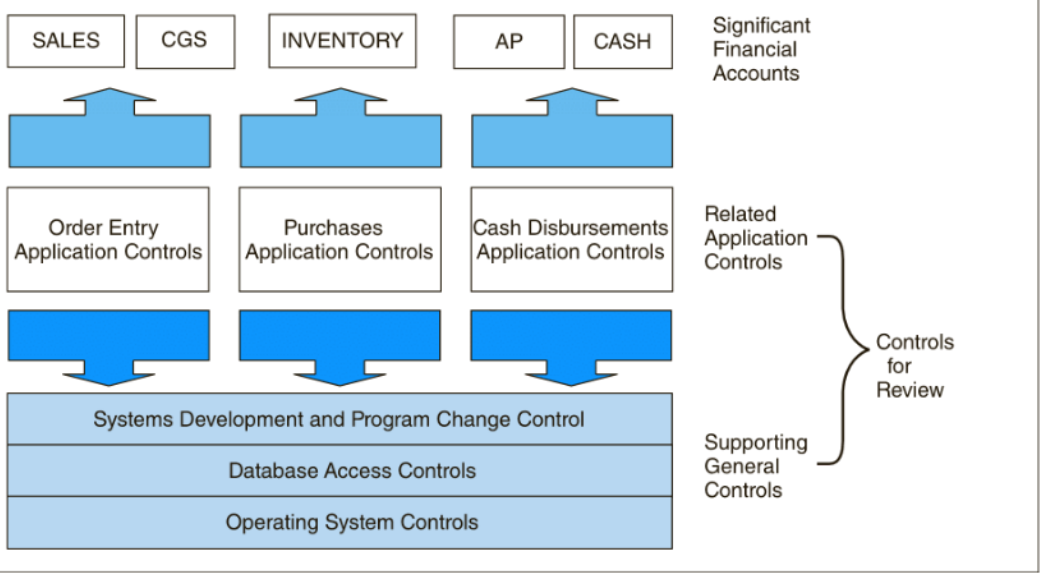
AUDIT IMPLICATIONS OF SECTIONS 302 AND 404

Prior to SOX, external auditors were not required to test internal controls as part of their attest function. They were required to be familiar with the client organization's internal controls but had the option of not relying on them and thus not performing tests of controls. The audit could, and often did, therefore consist primarily of substantive tests.

SOX legislation dramatically expands the role of external auditors by mandating that they attest to the quality of internal controls. This constitutes the issuance of a separate audit opinion in addition to the opinion on the fairness of the financial statements. The standard for this additional audit opinion is high. Indeed, the auditor is precluded from issuing an unqualified opinion if only one material weakness in internal control is detected. As explained in the previous section, a qualified opinion on internal controls does not necessarily mean a qualified opinion on the financial statements. Auditors are permitted to simultaneously render a qualified opinion on controls and an unqualified opinion on the financial statements when they conclude through substantive tests that the control weakness(es) did not cause the financial statements to be materially misrepresented.

As part of the attestation responsibility, PCAOB Standard No. 5 specifically requires auditors to understand transaction flows, including the controls pertaining to how transactions are initiated, authorized, recorded, and reported. This involves first selecting the financial accounts that have material implications for financial reporting and identifying the application controls related to those accounts. As previously noted, the reliability of application controls rests on the IT general controls that support them. These include controls over access to databases, operating systems, and networks. The sum of these controls, both application and general, constitute the relevant internal controls over financial reporting that need to be reviewed. Figure 15-2 illustrates this IT control relationship.

FIGURE 15-2 INFORMATION TECHNOLOGY CONTROL RELATIONSHIP



Compliance with Section 404 requires management to provide the external auditors with documented evidence of functioning controls related to selected material accounts in its report on control effectiveness. The organization's internal audit function, or a specialized SOX group, would likely perform these tests.

Section 302 also carries significant auditor implications. In addition to expressing an opinion on the effectiveness of internal control, auditors have responsibility regarding management's quarterly certifications of internal controls. Specifically, auditors must perform the following procedures quarterly to identify any material modifications in controls over financial reporting:

- Interview management regarding any significant changes in the design or operation of internal control that occurred subsequent to the preceding annual audit or prior review of interim financial information.
- Evaluate the implications of misstatements identified by the auditor as part of the interim review that relate to effective internal controls.
- Determine whether changes in internal controls are likely to materially affect internal control over financial reporting.

Finally, SOX places responsibility on auditors to detect fraudulent activity and emphasizes the importance of controls designed to prevent or detect fraud that could lead to material misstatement of the financial statements. Management is responsible for implementing such controls, and auditors are specifically required to test them. Because computers lie at the heart of the modern organizations' accounting and financial reporting systems, the topic of **computer fraud** falls within the management and audit responsibilities specified by SOX. The following section deals with several computer fraud issues.

Computer Fraud

We saw in Chapter 3 that fraud loss estimates for 2012 are $3.5 trillion. How much of this can be traced to computer fraud is difficult to say. One reason for uncertainty is that computer fraud is not well defined. For example, we saw in the ethics section of Chapter 3 that some people consider copying commercial computer software to be neither unethical nor illegal. On the other side of this issue, software vendors consider such acts to be criminal. Regardless of how narrowly or broadly computer fraud is defined, it is a rapidly growing phenomenon. For purposes of our discussion, computer fraud includes:

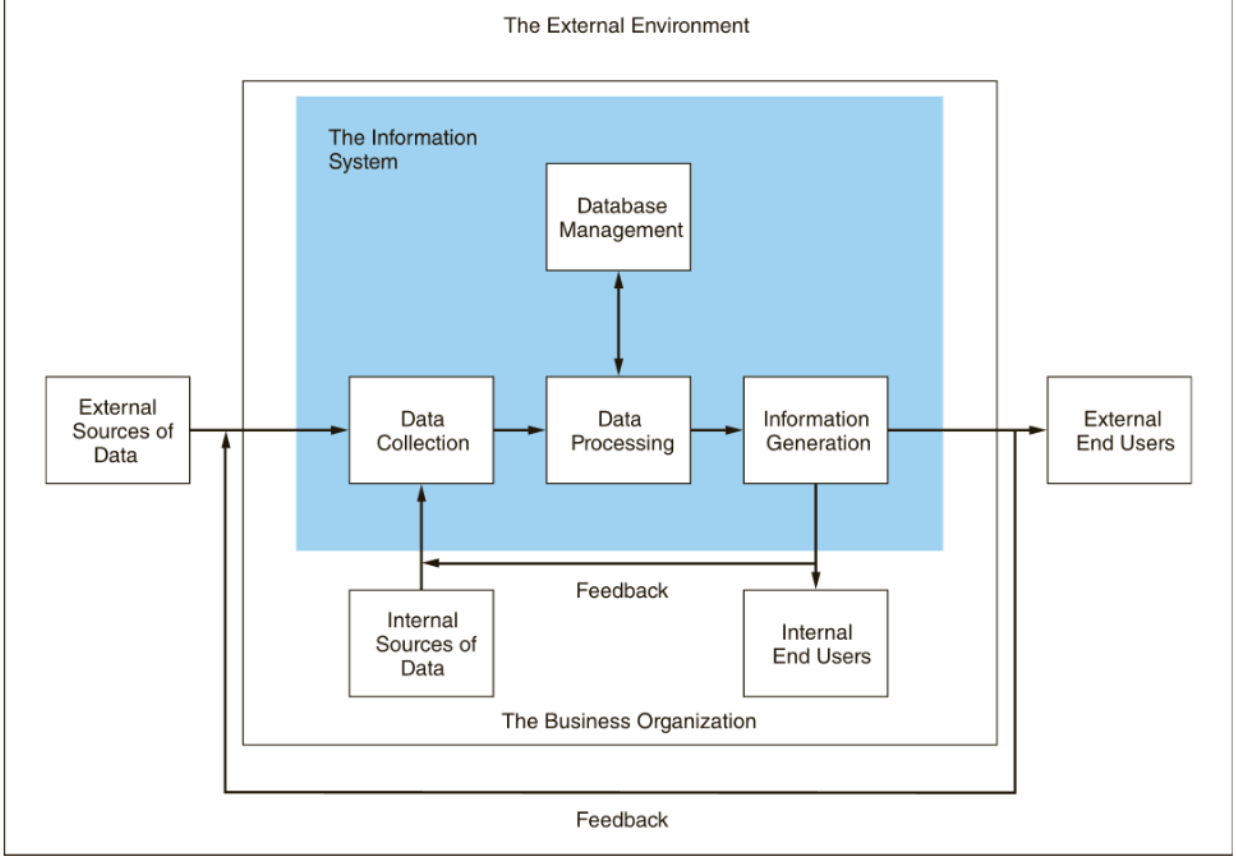
- The theft, misuse, or misappropriation of assets by altering computer-readable records and files.
- The theft, misuse, or misappropriation of assets by altering the logic of computer software.
- The theft or illegal use of computer-readable information.
- The theft, corruption, illegal copying, or intentional destruction of computer software.
- The theft, misuse, or misappropriation of computer hardware.

The general model for accounting information systems shown in Figure 15-3 conceptually portrays the key stages of an information system.[7] Each stage in the model—data collection, data processing, database management, and information generation—is a potential area of risk for certain types of computer fraud. In this section, we examine only the general nature of the risks; specific control techniques needed to reduce the risks are discussed later in this chapter and in the remaining two chapters.

DATA COLLECTION. Data collection is the first operational stage in the information system. The control objective is to ensure that event data entering the system are valid, complete, and free from material errors. In many respects, this is the most important stage in the system. Should erroneous or fraudulent transactions pass through data collection undetected, the organization runs the risk that the system will process the transaction and that it will impact the financial statements.

7 This model was introduced in Chapter 1.

FIGURE 15-3 THE GENERAL MODEL FOR ACCOUNTING INFORMATION SYSTEMS



The most common access point for perpetrating computer fraud is at the data collection stage. Frauds of this type require little or no computer skills on the part of the fraudster, but they do require poorly designed controls. The perpetrator need only understand how the system works and the control weaknesses of the system. The fraudulent act involves entering falsified data into the system. This may involve deleting, altering, or creating a transaction. For example, to commit payroll fraud, the perpetrator may insert a fraudulent payroll transaction along with legitimate transactions. Unless internal controls are in place to detect the insertion, the system will generate an additional paycheck for the perpetrator. A variation on this type of fraud is to change the Hours Worked field in an otherwise legitimate payroll transaction to increase the amount of the paycheck.

Still another variant of this fraud is to disburse cash in payment of a false account payable. By entering fraudulent supporting documents (purchase order, receiving report, and supplier invoice) at the data collection stage of the accounts payable system, a perpetrator can fool the system into creating an accounts payable record for a nonexistent purchase. Once the record is created, the system will presume it is legitimate and, on the due date, disperse funds to the perpetrator in payment of a bogus liability.

Networked systems expose organizations to transaction frauds from remote locations. Masquerading, piggybacking, and hacking are examples of such fraud techniques. Masquerading involves a perpetrator gaining access to the system from a remote site by pretending to be an authorized user. This usually requires first gaining authorized access to a password. Piggybacking is a technique in which the perpetrator at a remote site taps in to the telecommunications lines and latches on to an authorized user who is logging in to the system. Once in the system, the

perpetrator can masquerade as the authorized user. Hacking may involve piggybacking or masquerading techniques. Hackers are distinguished from other computer criminals because their motives are not usually to defraud for financial gain. More often, they are motivated by the challenge of breaking into the system rather than the theft of assets. Nevertheless, hackers have caused extensive damage and loss to organizations by destroying and corrupting corporate data.

DATA PROCESSING. Once collected, data usually require processing to produce information. Tasks in data processing include mathematical algorithms (such as linear programming models) used for production scheduling applications, statistical techniques for sales forecasting, and posting and summarizing procedures used for accounting applications. Data processing frauds fall into two classes: program fraud and operations fraud.

Program fraud includes the following techniques: (1) creating illegal programs that can access data files to alter, delete, or insert values into accounting records; (2) destroying or corrupting a program's logic using a computer virus; or (3) altering program logic to cause the application to process data incorrectly. For example, the program a bank uses to calculate interest on its customers' accounts typically will produce rounding errors because the precision of the interest calculation is greater than the reporting precision. Therefore, interest figures that are calculated to several decimal places produce values to a fraction of one cent and must be rounded to whole numbers for reporting purposes. Interest calculation programs typically have a standard rounding routine to keep track of the rounding errors so that the total interest charge to the bank equals the sum of the individual credits. This involves temporarily placing fractional amounts left over from each calculation in an internal memory accumulator. When the amount in the accumulator totals one cent (plus or minus), the penny is added to the specific customer's account that is being processed at that time. In other words, one cent is added to (or deducted from) customer accounts randomly. A form of program fraud called the salami fraud involves modifying the rounding logic of the program so it no longer adds the one cent randomly. Instead, the modified program always adds the plus cent to the perpetrator's account, but it still adds the minus cent randomly. This can divert a considerable amount of cash to the perpetrator, but the accounting records stay in balance to conceal the crime.

Operations fraud is the misuse or theft of the firm's computer resources. This often involves using the computer to conduct personal business. For example, a programmer may use the firm's computer time to write software that he sells commercially. A CPA in the controller's office may use the company's computer to prepare tax returns and financial statements for her private clients. Similarly, a corporate lawyer with a private practice on the side may use the firm's computer to search for court cases and decisions in commercial databases. The cost of accessing the database is charged to the organization and hidden among legitimate charges.

DATABASE MANAGEMENT. The organization's database is its physical repository for financial and nonfinancial data. **Database management fraud** includes altering, deleting, corrupting, destroying, or stealing an organization's data. Because access to database files is an essential element of this fraud, it is often associated with transaction or program fraud. A common fraud technique is to access the database from a remote site and browse the files for useful information that can be copied and sold to competitors.

Disgruntled employees have been known to destroy company data files simply to harm the organization. One method is to insert a destructive routine called a logic bomb into a program. At a specified time, or when certain conditions are met, the logic bomb erases the data files that the program accesses. For example, a disgruntled programmer who is contemplating leaving an organization inserts a logic bomb into the payroll system. Weeks later, when the system detects that the programmer's name has been removed from the payroll file, the logic bomb is activated and erases the entire payroll file.

INFORMATION GENERATION. Information generation is the process of compiling, arranging, formatting, and presenting information to users. Information can be an operational document such as a sales order, a report sent to a computer screen, or published financial statements.

A common form of computer fraud at the information generation stage is to steal, misdirect, or misuse computer output. One low-tech but effective technique called **scavenging** involves searching through the trash of the computer center for discarded output. Sometimes, output reports that are misaligned on the paper or slightly garbled during printing are discarded into the trash. A perpetrator may obtain useful information from hard-copy reports that were rejected during processing.

Another form of fraud called **eavesdropping** involves listening to output transmissions over telecommunication lines. Technologies are readily available that enable perpetrators to intercept messages being sent over unprotected telephone lines and microwave channels. Most experts agree that it is practically impossible to prevent a determined perpetrator from accessing data communication channels. Data encryption, however, can render useless any data captured in this **way.**

With this backdrop in place, the scene is set for viewing control techniques and tests of controls that might be required under SOX. PCAOB Auditing Standard No. 5 emphasizes that management and auditors use a risk-based approach rather than a one-size-fits-all approach to the design and assessment of controls. In other words, the size and complexity of the organization needs to be considered in determining the nature and extent of controls that are necessary. The reader should recognize, therefore, that the controls presented in the remainder of this chapter and in the following two chapters describe the needs of a generic organization and may not apply in specific situations.

IT Governance Controls

IT governance is a broad concept relating to the decision rights and accountability for encouraging desirable behavior in the use of IT. Although important, not all elements of IT governance relate specifically to control issues that SOX addresses and that are outlined in the COSO framework. In this chapter, we consider three governance issues that do organizational structure of the IT function, computer operations, and disaster recovery planning.

The discussion of each of these governance issues begins with an explanation of the nature of risk and a description of the controls needed to mitigate the risk. Then, the audit objective is presented. This establishes what needs to be verified regarding the function of the control in place. Finally, example tests of controls are offered that describe how auditors might gather evidence to satisfy the audit objective. These control objectives and associated tests may be performed by internal auditors providing evidence of management's compliance with SOX or by external auditors as part of their attest function. In this regard, we make no distinction between the two roles.

Organizational Structure Controls

Previous chapters have stressed the importance of segregating incompatible duties within manual activities. Specifically, operational tasks should be separated to:

1. Segregate the task of transaction authorization from transaction processing.
2. Segregate record keeping from asset custody.
3. Divide transaction-processing tasks among individuals so that fraud will require collusion between two or more individuals.

The tendency in an IT environment is to consolidate activities. A single application may authorize, process, and record all aspects of a transaction. Thus, the focus of segregation control shifts from the operational level (transaction processing tasks that computer programs now perform) to higher-level organizational relationships within the IT function. The interrelationships among systems development, application maintenance, database administration, and computer operations activities are of particular concern.

The following section examines organizational control issues within the context of two generic models—the centralized model and the distributed model. For discussion purposes, these are presented as alternative structures; in practice, the IT environments of most firms possess elements of both.

SEGREGATION OF DUTIES WITHIN THE CENTRALIZED FIRM

Figure 15-4 presents an organizational chart of a centralized IT function. A similar organizational chart was presented in Chapter 1 to provide the basis for discussing IT tasks. It is reexamined here to study the control objectives behind separating these tasks. If the positions represented in this chart are unfamiliar, you should review the relevant sections in Chapter 1 before continuing.

Separating Systems Development from Computer Operations

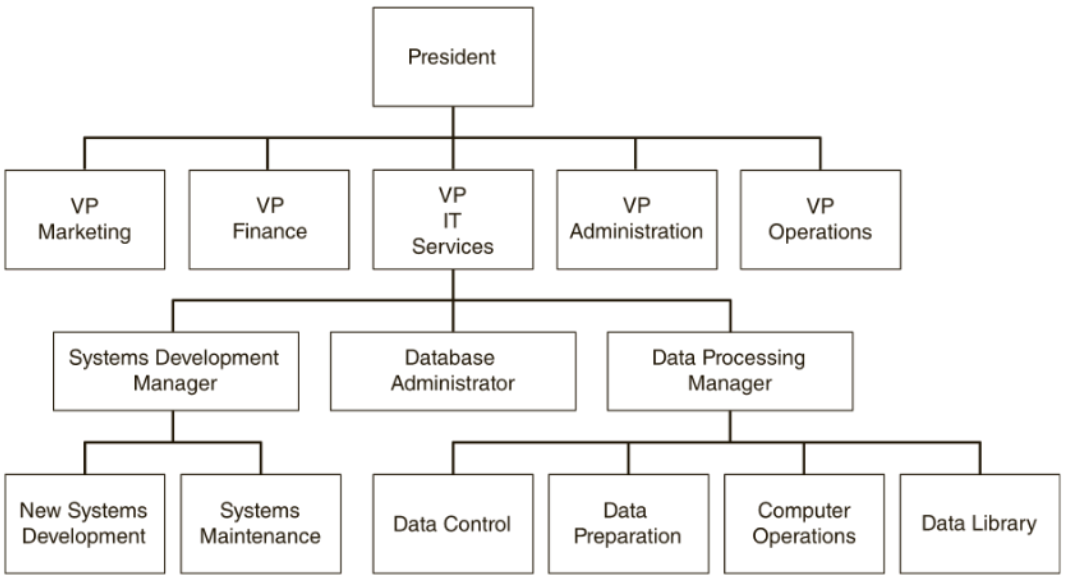
The segregation of systems development (both new systems development and maintenance) and operations activities is of great importance. The responsibilities of these groups should not be commingled. Systems development and maintenance professionals acquire (by in-house development and purchase) and maintain systems for users. Operations staff should run these systems and have no involvement in their design and implementation. Consolidating these functions invites fraud. With detailed knowledge of an application's logic and control parameters along with access to the computer operations, an individual could make unauthorized changes to application logic during program execution. Such changes may be temporary (on the fly) and will disappear with little or no trace when the application terminates.

Separating the Database Administrator from Other Functions

Another important organizational control is the segregation of the database administrator (DBA) function from other IT functions. The DBA is responsible for a number of critical tasks pertaining to database security, including creating the database schema, creating **user views** (subschemas), assigning access authority to users, monitoring database usage, and planning for future expansion. Delegating these responsibilities to others who perform incompatible tasks threatens database integrity. Figure 15-4 shows how the DBA function is organizationally independent.

SEPARATING THE DBA FROM SYSTEMS DEVELOPMENT. Programmers create applications that access, update, and retrieve data from the database. Chapter 9 illustrated how database

FIGURE 15-4 ORGANIZATIONAL CHART OF A CENTRALIZED INFORMATION TECHNOLOGY FUNCTION



access control is achieved through the creation of user views, which is a DBA responsibility. To achieve database access, therefore, both the programmer and the DBA need to agree as to the attributes and tables (the user view) to make available to the application (or user) in question. If done properly, this permits and requires a formal review of the user data needs and security issues surrounding the request. Assigning responsibility for user view definition to individuals with programming responsibility removes this need to seek agreement and thus effectively erodes **access controls** to the DBMS.

Separating New Systems Development from Maintenance

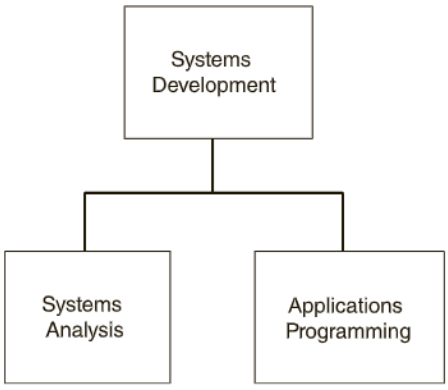
Some companies organize their systems development function into two groups: systems analysis and programming. This organizational alternative is presented in Figure 15-5. The systems analysis group works with the user to produce a detailed design of the new system. The programming group codes the programs according to these design specifications. Under this approach, the programmer who codes the original programs also maintains them during the maintenance phase of the systems development life cycle. Although a popular arrangement, this approach promotes two potential problems: inadequate documentation and fraud.

INADEQUATE DOCUMENTATION. Poor-quality systems documentation is a chronic IT problem and a significant challenge for many organizations seeking SOX compliance. There are at least two explanations for this phenomenon. First, documenting systems is not as interesting as designing, testing, and implementing them. Systems professionals much prefer to move on to an exciting new project rather than document one just completed.

The second possible reason for poor documentation is job security. When a system is poorly documented, it is difficult to interpret, test, and debug. Therefore, the programmer who understands the system (the one who coded it) maintains bargaining power and becomes relatively indispensable. When the programmer leaves the firm, however, a new programmer inherits maintenance responsibility for the undocumented system. Depending on its complexity, the transition period may be long and costly.

PROGRAM FRAUD. When the original programmer of a system is also assigned maintenance responsibility, the potential for fraud is increased. Program fraud involves making unauthorized changes to program modules for the purpose of committing an illegal act. The original programmer may have successfully concealed fraudulent code among the thousands of lines of legitimate code and the hundreds of modules that constitute a system. For the fraud to work successfully,

FIGURE 15-5 ALTERNATIVE ORGANIZATION OF SYSTEMS DEVELOPMENT



however, the programmer must be able to control the situation through exclusive and unrestricted access to the application's programs. The programmer needs to protect the fraudulent code from accidental detection by another programmer performing maintenance or by auditors testing application controls. Therefore, having sole responsibility for maintenance is an important element in the duplicitous programmer's scheme. Through this maintenance authority, the programmer may freely access the system, disabling fraudulent code during audits and then restoring the code when the coast is clear. Frauds of this sort may continue for years without detection.

A Superior Structure for Systems Development

Figure 15-4 presents a superior organizational structure in which the systems development function is separated into two independent groups: new systems development and systems maintenance. The new systems development group is responsible for designing, programming, and implementing new systems projects. Upon successful implementation, responsibility for the system's ongoing maintenance falls to the systems maintenance group. This structure helps resolve the two control problems described previously.

First, documentation standards are improved because the maintenance group will require adequate documentation to perform their maintenance duties. Without complete documentation, the formal transfer of system responsibility from new systems development to systems maintenance cannot occur.

Second, denying the original programmer future access to the application code deters program fraud. Fraudulent code within an application, which is out of the perpetrator's control, increases the risk that the fraud will be discovered. The success of this control depends on the existence of other controls that limit, prevent, and detect unauthorized access to programs. These controls are discussed in Chapter 17. Although organizational separations alone cannot guarantee that computer frauds will not occur, they are critical to creating the control environment needed to reduce the risk.

THE DISTRIBUTED MODEL

An alternative to the centralized model is the concept of **distributed data processing (DDP)**. The topic of DDP is quite broad, touching on such related topics as end-user computing, commercial software, networking, and office automation. Simply stated, DDP involves reorganizing the IT function into small units that are distributed to end users and placed under their control. Any or all of the IT activities represented in Figure 15-4 may be distributed. Figure 15-6 shows a possible new organizational structure following the distribution of all data processing tasks to the end-user areas.

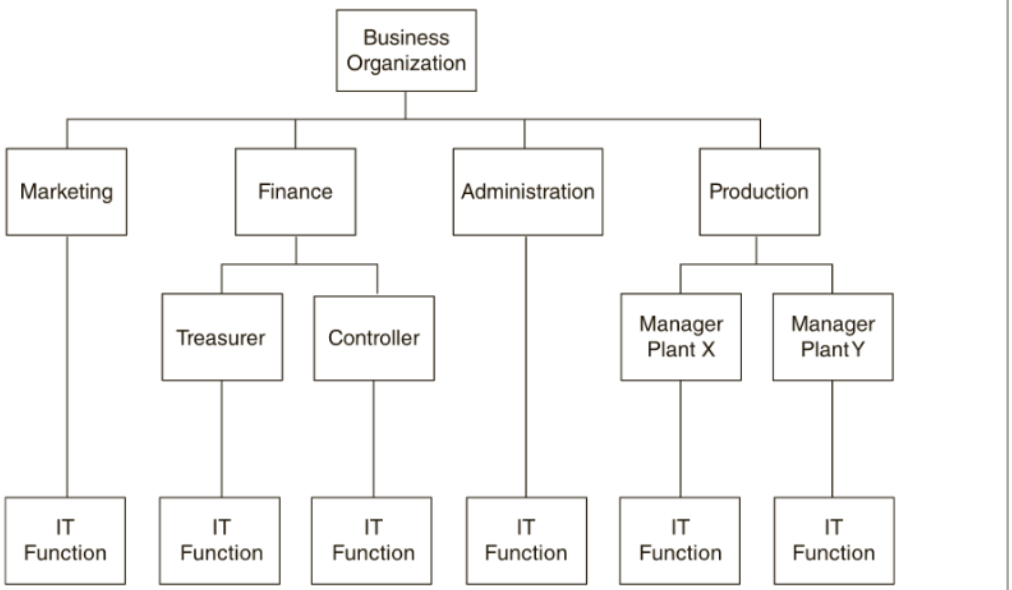
Notice that the central IT function has been eliminated from the organizational structure. Individual IT units now perform this role. In recent years, **DDP** has become an economic and operational feasibility that has revolutionized business operations. However, DDP is a mixed bag of advantages and disadvantages.

Advantages of DDP

The most commonly cited advantages of DDP are related to cost savings, increased user satisfaction, and improved operational efficiency. Specific issues are discussed in the following section.

COST REDUCTIONS. Achieving economies of scale is the principal justification for the centralized approach. The economics of data processing favored large, expensive, powerful computers. The wide variety of needs that such centralized systems had to satisfy called for computers that were highly generalized and that employed complex operating systems. Powerful yet inexpensive small-scale computer systems, which can cost-effectively perform specialized functions, have changed the economics of data processing dramatically. In addition, the unit cost of data storage, which was once the justification for consolidating data in a central location, is no longer a prime consideration. Moreover, the move to **DDP** can reduce costs in two other areas: (1) data can be entered and edited locally, thus eliminating the centralized tasks of data conversion and data

FIGURE 15-6 ORGANIZATIONAL STRUCTURE FOR A DISTRIBUTED SYSTEM



control, and (2) application complexity can be reduced, which in turn reduces development and maintenance costs.

IMPROVED COST CONTROL RESPONSIBILITY. Managers assume responsibility for the financial success of their operations. This requires that they be properly empowered with the authority to make decisions about resources that influence their overall success. Therefore, if information-processing capability is critical to the success of a business operation, then should management not be given control over these resources?

IMPROVED USER SATISFACTION. Perhaps the most often cited benefit of DDP is improved user satisfaction. This derives from three areas of need that too often go unsatisfied in the centralized approach: (1) as previously stated, users desire to control the resources that influence their profitability, (2) users want systems professionals (analysts, programmers, and computer operators) who are responsive to their specific situation, and (3) users want to become more actively involved in developing and implementing their own systems. Proponents of DDP argue that providing more customized support—feasible only in a distributed environment—has direct benefits for user morale and productivity.

BACKUP. The final argument in favor of DDP is the ability to back up computing facilities to protect against potential disasters such as fires, floods, sabotage, and earthquakes. One solution is to build excess capacity into each IT unit. If a disaster destroys a single site, its transactions can be processed by the other sites. This requires close coordination between decision makers to ensure that they do not implement incompatible hardware and software at their sites.

Disadvantages of DDP

This discussion focuses on important issues that carry control implications that accountants should recognize. The loss of control is one of the most serious disadvantages of DDP. Other potential problems include the inefficient use of resources, the destruction of audit trails,

inadequate segregation of duties, an increased potential for programming errors and systems failures, and the lack of standards. Specific problems are examined in the following section.

MISMANAGEMENT OF ORGANIZATION-WIDE RESOURCES. Some argue that when organization-wide resources exceed a threshold amount, say, 5 percent of the total operations budget, the resources should be controlled and monitored centrally. This argument counters the argument presented earlier favoring the distribution of organization-wide resources. Information-processing services (such as computer operations, programming, data conversion, and database management) represent a significant expenditure for many organizations. Those opposed to DDP argue that distributing responsibility for these resources will inevitably lead to their mismanagement and suboptimal utilization.

HARDWARE AND SOFTWARE INCOMPATIBILITY. Distributing the responsibility for hardware and software purchases to user management can result in uncoordinated and poorly conceived decisions. Working independently, decision makers may settle on dissimilar and incompatible operating systems, technology platforms, spreadsheet programs, word processors, and database packages. Such hardware and software incompatibilities can degrade and disrupt communications between organizational units.

REDUNDANT TASKS. Autonomous systems development activities distributed throughout the firm can result in each user area reinventing the wheel. For example, application programs created by one user, which could be used with little or no change by others, will be redesigned from scratch rather than shared. Likewise, data common to many users may be recreated for each of them, resulting in a high level of data redundancy.

CONSOLIDATING INCOMPATIBLE ACTIVITIES. The distribution of the IT function to individual user areas results in the creation of many very small units that may not permit the necessary separation of incompatible functions. For example, within a single IT unit, the same person may program applications, perform program maintenance, enter transaction data into the computer, and operate the computer equipment. This situation represents a fundamental violation of internal control.

HIRING QUALIFIED PROFESSIONALS. End-user managers may lack the knowledge to evaluate the technical credentials and relevant experience of candidates applying for a position as a computer professional. Also, if the organizational unit into which a new employee is entering is small, the opportunity for personal growth, continuing education, and promotion may be limited. For these reasons, end-user managers sometimes experience difficulty attracting highly qualified personnel, which increases the risk of programming errors and systems failures.

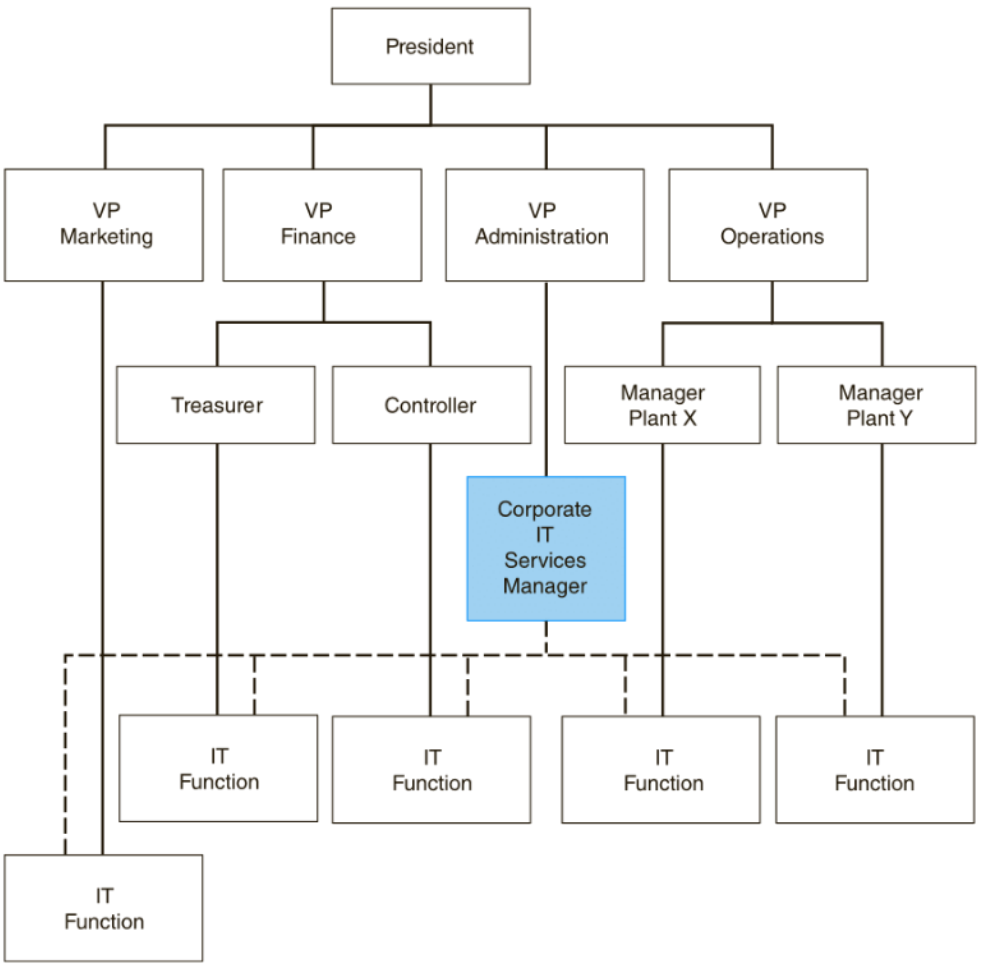
LACK OF STANDARDS. Because of the distribution of responsibility in the DDP environment, standards for developing and documenting systems, choosing programming languages, acquiring hardware and software, and evaluating performance may be unevenly applied or nonexistent. Opponents of DDP argue that the risks associated with the design and operation of a data processing system is made tolerable only if such standards are consistently applied. This requires that standards be imposed centrally.

CREATING A CORPORATE IT FUNCTION

The completely centralized and the fully distributed models represent extreme positions on a continuum of structural alternatives. The needs of most firms fall somewhere between these end points. For these firms, the control problems associated with DDP can, to some extent, be overcome by implementing a **corporate IT function**. Figure 15-7 illustrates this organizational approach.

The corporate IT function is a leaner unit with a mission different from that of the centralized IT function shown in Figure 15-4. This group provides technical advice and expertise to the

FIGURE 15-7 DISTRIBUTED ORGANIZATION WITH CORPORATE IT FUNCTION



various distributed IT functions, as the dotted lines represent in Figure 15-7. Some of the support services provided are described in the following section.

Central Testing of Commercial Software and Hardware

The corporate IT group is better able to evaluate the merits of competing vendor software and hardware. A central, technically astute group such as this can evaluate systems features, controls, and compatibility with industry and organizational standards most efficiently. After testing, they can make recommendations to user areas for guiding acquisition decisions.

User Services

A valuable feature of the corporate group is its user services function. This activity provides technical help to users during the installation of new software and in troubleshooting hardware and software problems. The creation of an electronic bulletin board for users is an excellent way to distribute information about common problems and allows the sharing of user-developed programs with others in the organization. User services staff often teach technical courses for end users, which raises the level of user awareness and promotes the continued education of technical personnel.

Standard-Setting Body

Establishing central guidance can improve the relatively poor control environment common to the distributed model. The corporate group can establish and distribute to user areas appropriate standards for systems development, programming, and documentation that will be compliant with SOX requirements.

Personnel Review

The corporate group is better equipped than users to evaluate the technical credentials of prospective systems professionals. Although the prospective IT hires will work for the distributed user groups, the involvement of the corporate group in hiring decisions can render a valuable service to the organization.

AUDIT OBJECTIVES RELATING TO ORGANIZATIONAL STRUCTURE

The auditor's objective is to ascertain whether individuals serving in incompatible areas are segregated in accordance with an acceptable level of risk and in a manner that promotes an effective working environment.

AUDIT PROCEDURES RELATING TO ORGANIZATIONAL STRUCTURE

The following audit tests would provide evidence to achieve the audit objective.

- Obtain and review the corporate policy on computer security. Verify that the security policy is communicated to responsible employees and supervisors.
- Review relevant documentation, including the current organizational chart, mission statement, and job descriptions for key functions, to determine if individuals or groups are performing incompatible functions.
- Review systems documentation and maintenance records for a sample of applications. Verify that maintenance programmers assigned to specific projects are not also the original design programmers.
- Through observation, determine that the segregation policy is being followed in practice. Review operations room access logs to determine whether programmers enter the facility for reasons other than system failures.
- Review user roles to verify that programmers have access privileges consistent with their job descriptions.

Computer Center Security and Controls

Fires, floods, wind, sabotage, earthquakes, or even power outages can deprive an organization of its data processing facilities and bring to a halt those functions that are performed or aided by computer. Although the likelihood of such a disastrous event is remote, the consequences to the organization could be serious. If a disaster occurs, the organization not only loses its investment in data processing facilities, but more importantly, it also loses its ability to do business.

The objective of this section is to present computer center controls that help create a secure environment. We will begin with a look at controls designed to prevent and detect threats to the computer center. However, no matter how much is invested in control, some disasters simply cannot be anticipated and prevented. What does a company do to prepare itself for such an event? How will it recover? These questions are at the heart of the organization's disaster recovery plan. The next section deals specifically with issues pertaining to the development of a disaster recovery plan.

COMPUTER CENTER CONTROLS

Weaknesses in computer center security have a potential impact on the function of application controls related to the financial reporting process. Therefore, this physical environment is a control issue for SOX compliance. The following are some of the control features that contribute directly to computer center security.

Physical Location

The physical location selected for a computer center can influence the risk of disaster. To the extent possible, the computer center should be located away from human-made and natural hazards, such as processing plants, gas and water mains, airports, high-crime areas, flood plains, and geological faults.

Construction

Ideally, a computer center should be located in a single-story building of solid construction with controlled access (discussed in the following section). Utility (power and telephone) and communications lines should be underground. The building windows should not open. An air filtration system should be in place that is capable of excluding pollens, dust, and dust mites.

Access

Access to the computer center should be limited to the operators and other employees who work there. Programmers and analysts who occasionally need to correct program errors should be required to sign in and out. The computer center should maintain accurate records of all such events to verify the function of access control. The main entrance to the computer center should be through a single door, although fire exits with alarms are necessary. To achieve a higher level of security, closed-circuit cameras and video recording systems should monitor access.

Air Conditioning

Computers function best in an air-conditioned environment. For mainframe computers, providing adequate air conditioning is often a requirement of the vendor's warranty. Computers operate best in a temperature range of 70 to 75 degrees Fahrenheit and a relative humidity of 50 percent. Logic errors can occur in computer hardware when temperatures depart significantly from this range. Also, the risk of circuit damage from static electricity is increased when humidity drops. High humidity, on the other hand, can cause molds to grow and paper products (such as source documents) to swell and jam equipment.

Fire Suppression

The most common threat to a firm's computer equipment is fire. Half of the companies that suffer fires go out of business because of the loss of critical records, such as accounts receivable. The implementation of an effective fire-suppression system requires consultation with specialists. Some of the major features of such a system are listed in the following section.

1. Automatic and manual alarms should be placed in strategic locations around the installation. These alarms should be connected to a permanently staffed firefighting station.
2. There must be an automatic fire-extinguishing system that dispenses the appropriate type of suppressant (carbon dioxide or halon) for the location. For example, spraying water and certain chemicals on a computer can do as much damage as the fire.
3. Manual fire extinguishers should be placed at strategic locations.
4. The building should be of sound construction to withstand water damage that fire-suppression equipment causes.
5. Fire exits should be clearly marked and illuminated during a fire.

Fault Tolerance Controls

Fault tolerance is the ability of the system to continue operation when part of the system fails because of hardware failure, application program error, or operator error. Implementing redundant system components can achieve various levels of fault tolerance. Redundant disks and power supplies are two common examples.

Redundant arrays of independent disks (RAID) *involves using parallel disks that contain redundant elements of data and applications. If one disk fails, the lost data are automatically reconstructed from the redundant components stored on the other disks.*

Uninterruptible power supplies *help prevent data loss and system corruption. In the event of a power supply failure, short-term backup power is provided to allow the system to shut down in a controlled manner. Implementing fault tolerance control ensures that there is no single point of potential system failure. Total failure can occur only in the event of the failure of multiple components.*

Audit Objectives Relating to Computer Center Security

The audit objectives are to determine whether: (1) controls governing computer center security are adequate to reasonably protect the organization from physical damage or losses; (2) insurance coverage on equipment is adequate to compensate the organization for the destruction of, or damage to, its computer center; and (3) operator documentation is adequate to deal with system failures as well as routine operations.

Audit Procedures for Assessing Physical Security Controls

The following are tests of physical security controls.

TESTS OF PHYSICAL CONSTRUCTION. The auditor should obtain architectural plans to determine that the computer center is solidly built of fireproof material. There should be adequate drainage under the raised floor to allow water to flow away in the event of water damage from a fire in an upper floor or from some other source. In addition, the auditor should assess the physical location of the computer center. The facility should be located in an area that minimizes its exposure to fire, civil unrest, and other hazards.

TESTS OF THE FIRE DETECTION SYSTEM. The auditor should establish that fire detection and suppression equipment, both manual and automatic, are in place and are tested regularly. The fire detection system should detect smoke, heat, and combustible fumes. The evidence may be obtained by reviewing official fire marshal records of tests, which are stored at the computer center.

TESTS OF ACCESS CONTROL. The auditor must establish that routine access to the computer center is restricted to authorized employees. Details about visitor access (by programmers and others), such as arrival and departure times, purpose, and frequency of access, can be obtained by reviewing the access log. To establish the veracity of this document, the auditor may covertly observe the process by which access is permitted.

Tests of Fault Tolerance Controls

RAID. Many RAID configurations provide a graphical mapping of their redundant disk storage. From this mapping, the auditor should determine if the level of RAID in place is adequate for the organization, given the level of business risk associated with disk failure. If the organization is not employing RAID, the potential for a single point of system failure exists. The auditor should review with the system administrator alternative procedures for recovering from a disk failure.

POWER SUPPLIES BACKUP. The auditor should verify from test records that computer center personnel perform periodic tests of the backup power supply to ensure that it has sufficient

capacity to run the computer and air conditioning. These important tests and their results should be formally recorded.

Audit Procedures for Verifying Insurance Coverage

The auditor should annually review the organization's insurance coverage on its computer hardware, software, and physical facility. The auditor should verify that all new acquisitions are listed on the policy and that obsolete equipment and software have been deleted. The insurance policy should reflect management's needs in terms of extent of coverage. For example, the firm may wish to be partially self-insured and require minimum coverage. On the other hand, the firm may seek complete replacement-cost coverage.

Audit Procedures for Verifying Adequacy of Operator Documentation

Computer operators use documentation called a run manual to run certain aspects of the system. In particular, large batch systems often require special attention from operators. During the course of the day, computer operators may execute dozens of computer programs, each of which might process multiple files and produce multiple reports. To achieve effective data processing operations, the run manual must be sufficiently detailed to guide operators in their tasks. The auditor should review the run manual for completeness and accuracy. The typical contents of a run manual include:

- The name of the system, such as "Purchases System"
- The run schedule (daily, weekly, time of day)
- Required hardware devices (tapes, disks, printers, or special hardware)
- File requirements specifying all the transaction (input) files, master files, and output files used in the system
- Run-time instructions describing the error messages that may appear, actions to be taken, and the name and telephone number of the programmer on call, should the system fail
- A list of users who receive the output from the run

Also, the auditor should verify that certain systems documentation, such as systems flowcharts, logic flowcharts, and program code listings, are not part of the operator's documentation. For reasons previously discussed, operators should not have access to the operational details of a system's internal logic.

Disaster Recovery Planning

Some disasters cannot be prevented or evaded. Recent events include hurricanes, widespread flooding, earthquakes, and the events of September 11, 2001. The survival of a firm affected by a disaster depends on how it reacts. With careful contingency planning, the full impact of a disaster can be absorbed, and the organization can still recover.

A **disaster recovery plan (DRP)** is a comprehensive statement of all actions to be taken before, during, and after a disaster, along with documented, tested procedures that will ensure the continuity of operations. Although the details of each plan are unique to the needs of the organization, all workable plans possess common features. The remainder of this section is devoted to a discussion of the following control issues: providing second-site backup, identifying critical applications, performing backup and **off-site storage** procedures, creating a disaster recovery team, and testing the DRP.

PROVIDING SECOND-SITE BACKUP

A necessary ingredient in a DRP is that it provides for duplicate data processing facilities following a disaster. The viable options available include the empty shell, recovery operations center, and internally provided backup.

The Empty Shell

The **empty shell** or cold site plan is an arrangement wherein the company buys or leases a building that will serve as a data center. In the event of a disaster, the shell is available and ready to receive whatever hardware the temporary user needs to run essential systems. This approach, however, has a fundamental weakness. Recovery depends on the timely availability of the necessary computer hardware to restore the data processing function. Management must obtain assurances (contracts) from hardware vendors that in the event of a disaster, the vendor will give priority to the company's computing needs. An unanticipated hardware supply problem at this critical juncture could be a fatal blow.

The Recovery Operations Center

A **recovery operations center (ROC)** or hot site is a fully equipped backup data center that many companies share. In addition to hardware and backup facilities, ROC service providers offer a range of technical services to their clients, who pay an annual fee for access rights. In the event of a major disaster, a subscriber can occupy the premises and, within a few hours, resume processing critical applications.

September 11, 2001, was a true test of the reliability and effectiveness of the ROC approach. Comdisco, a major ROC provider, had 47 clients who declared 93 separate disasters on the day of the attack. All 47 companies relocated and worked out of Comdisco's recovery centers. At one point, 3,000 client employees were working out of the centers. Thousands of computers were configured for clients' needs within the first 24 hours, and systems recovery teams were on-site wherever police permitted access. By September 25, nearly half of the clients were able to return to their facilities with a fully functional system.

A problem with this approach is the potential for competition among users for the ROC resources. A widespread natural disaster, such as a flood or an earthquake, may destroy the data processing capabilities of several ROC members located in the same geographic area. All the victims will find themselves vying for access to the same limited facilities. Because some ROC service providers oversell their capacity by a ratio of 20:1, the situation is analogous to a sinking ship that has an inadequate number of lifeboats.

The period of confusion following a disaster is not an ideal time to negotiate property rights. Therefore, before entering into an ROC arrangement, management should consider the potential problems of overcrowding and geographic clustering of the current membership.

Internally Provided Backup

Larger organizations with multiple data processing centers often prefer the self-reliance that creating internal excess capacity provides. This permits firms to develop standardized hardware and software configurations, which ensure functional compatibility among their data processing centers and minimize cutover problems in the event of a disaster.

Pershing, a division of Donaldson, Lufkin & Jenrette Securities Corporation, processes more than 36 million transactions per day, about 2,000 per second. Pershing management recognized that an ROC vendor could not provide the recovery time they wanted and needed. The company, therefore, built its own remote **mirrored data center**. The facility is equipped with high-capacity storage devices capable of storing more than 20 terabytes of data and two IBM mainframes running high-speed copy software. All transactions that the main system processes are transmitted in real time along fiber-optic cables to the remote backup facility. At any point in time, the mirrored data center reflects current economic events of the firm. The mirrored system has reduced Pershing's data recovery time from 24 hours to 1 hour.

IDENTIFYING CRITICAL APPLICATIONS

Another essential element of a DRP involves procedures to identify the critical applications and data files of the firm to be restored. Eventually, all applications and data must be restored to

pre-disaster business activity levels. Immediate recovery efforts, however, should focus on restoring those applications and data that are critical to the organization's short-term survival. In any disaster scenario, it is short-term survivability that determines long-term survival.

For most organizations, short-term survival requires the restoration of those functions that generate cash flows sufficient to satisfy short-term obligations. For example, assume that the following functions affect the cash flow position of a particular firm:

- Customer sales and service
- Fulfillment of legal obligations
- Accounts receivable maintenance and collection
- Production and distribution
- Purchasing
- Communications between branches or agencies
- Public relations

The computer applications that support these functions directly are critical. Hence, these applications should be so identified and prioritized in the restoration plan.

Application priorities may change over time, and these decisions must be reassessed regularly. Systems are constantly revised and expanded to reflect changes in user requirements. Similarly, the DRP must be updated to reflect new developments and identify critical applications. Up-to-date priorities are important because they affect other aspects of the strategic plan. For example, changes in application priorities may cause changes in the nature and extent of second-site backup requirements and specific backup procedures.

The task of identifying and prioritizing critical applications requires active participation of management, user departments, and internal auditors. Too often, this task is incorrectly perceived to be an IT issue and delegated to IT professionals. Although the technical assistance of systems personnel is required, this is primarily a business decision and those best equipped to understand the business problem should make it.

PERFORMING BACKUP AND OFF-SITE STORAGE PROCEDURES

All data files, application documentation, and supplies needed to perform critical functions should be specified in the DRP. Data processing personnel should routinely perform backup and storage procedures to safeguard these critical resources.

Backup Data Files

The state-of-the-art in database backup is the remote mirrored site, described previously, which provides complete data currency. Not all organizations are willing or able to invest in such backup resources. As a minimum, however, databases should be copied daily to tape or disks and secured off-site. In the event of a disruption, reconstruction of the database is achieved by updating the most current backup version with subsequent transaction data. Likewise, master files and transaction files should be protected.

Backup Documentation

The system documentation for critical applications should be backed up and stored off-site in much the same manner as data files. The large volumes of material involved and constant application revisions complicate the task. The process can be made more efficient through the use of computer-aided software engineering (CASE) documentation tools.

Backup Supplies and Source Documents

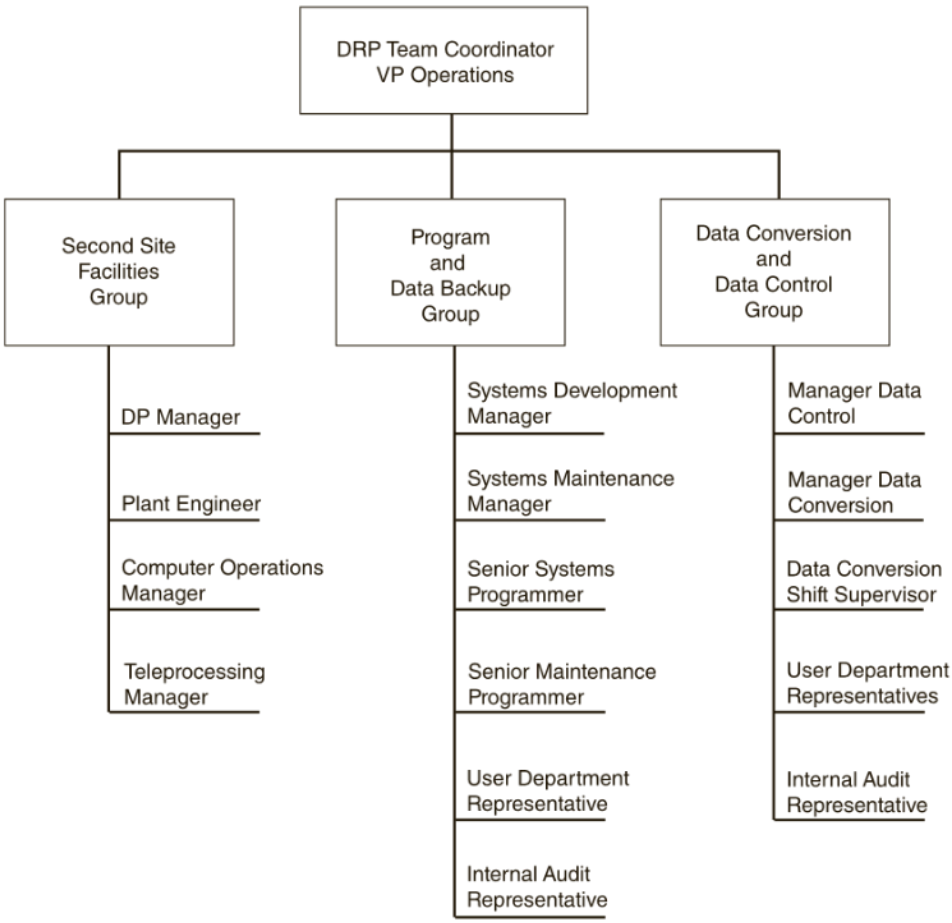
The firm should maintain backup inventories of supplies and source documents used in critical applications. Examples of critical supplies are check stocks, invoices, purchase orders, and any other special-purpose forms that cannot be obtained immediately.

CREATING A DISASTER RECOVERY TEAM

Recovering from a disaster depends on timely corrective action. Failure to perform essential tasks (such as obtaining backup files for critical applications) prolongs the recovery period and diminishes the prospects for a successful recovery. To avoid serious omissions or duplication of efforts during implementation of the contingency plan, individual task responsibility must be clearly defined and communicated to the personnel involved.

Figure 15-8 presents an organizational chart depicting the possible composition of a disaster recovery team. The team members should be experts in their areas and have assigned tasks. Following a disaster, team members will delegate subtasks to their subordinates. It should be noted that traditional control concerns do not apply in this setting. The environment the disaster creates may necessitate the breaching of normal controls such as segregation of duties, access controls, and supervision. At this point, business continuity is the primary consideration.

FIGURE 15-8 DISASTER RECOVERY TEAM



TESTING THE DRP

The most neglected aspect of contingency planning is testing of the plans. Nevertheless, DRP tests are important and should be performed periodically. Tests provide measures of the preparedness of personnel and identify omissions or bottlenecks in the plan.

A test is most useful in the form of a surprise simulation of a disruption. When the mock disaster is announced, the status of all processing that it affects should be documented. This provides a benchmark for subsequent performance assessments. The plan should be carried as far as is economically feasible. Ideally, this will include the use of backup facilities and supplies.

AUDIT OBJECTIVE: ASSESSING DISASTER RECOVERY PLANNING

The auditor should verify that management's disaster recovery plan is adequate and feasible for dealing with a catastrophe that could deprive the organization of its computing resources. The following tests focus on the areas of greatest concern.

AUDIT PROCEDURES FOR ASSESSING DISASTER RECOVERY PLANNING

Second-Site Backup

The auditor should evaluate the adequacy of the backup site arrangement. The client should possess vendor contracts guaranteeing timely equipment delivery to the cold site. In the case of ROC membership, the auditor should obtain information as to the total number of members and their geographic dispersion. A widespread disaster may create a demand that the backup facility cannot satisfy.

Critical Application List

The auditor should review the list of critical applications and ensure that it is up-to-date and complete. Missing applications may result in failure to recover. On the other hand, restoring noncritical applications diverts scarce resources to nonproductive tasks.

Backup Critical Applications and Critical Data Files

The auditor should verify that the organization has procedures in place to back up stored off-site copies of critical applications and data. Evidence of this can be obtained by selecting a sample of data files and programs and determining if they are being backed up as required.

Backup Supplies, Source Documents, and Documentation

The system documentation, supplies, and source documents needed to restore and run critical applications should be backed up and stored off-site. The auditor should verify that the types and quantities of items specified in the DRP exist in a secure location.

The Disaster Recovery Team

The DRP should clearly list the names, addresses, and emergency telephone numbers of the disaster recovery team members. The auditor should verify that members of the team are current employees and are aware of their assigned responsibilities. On one occasion, while reviewing a firm's DRP, the author discovered that a team leader listed in the plan had been deceased for nine months.

Outsourcing the IT Function

The costs, risks, and responsibilities associated with maintaining an effective corporate IT function are significant. Many executives have therefore opted to outsource their IT functions to third-party vendors who take over responsibility for the management of IT assets and staff and for delivery of IT services, such as data entry, data center operations, applications development,

applications maintenance, and network management. Often-cited benefits of **IT outsourcing** include improved core business performance, improved IT performance (because of the vendor's expertise), and reduced IT costs. By moving IT facilities offshore to low labor-cost areas and/or through economies of scale (by combining the work of several clients), the vendor can perform the outsourced function more cheaply than the client firm could have otherwise. The resulting cost savings are then passed to the client organization. Furthermore, many IT outsourcing arrangements involve the sale of the client firm's IT assets, both human and machine, to the vendor, which the client firm then leases back. This transaction results in a significant one-time cash infusion into the firm.

The logic underlying IT outsourcing follows from **core competency** theory, which argues that an organization should focus exclusively on its core business competencies, while allowing outsourcing vendors to efficiently manage the noncore areas such as the IT functions. This premise, however, ignores an important distinction between commodity and specific IT assets.

Commodity IT assets are not unique to a particular organization and are thus easily acquired in the marketplace. These include such things as network management, systems operations, server maintenance, and help-desk functions. As we saw in Chapter 12, even IT infrastructure and application software are provided as commodities through the cloud computing options of IaaS and SaaS, respectively. **Specific IT assets**, in contrast, are unique to the organization and support its strategic objectives. Because of their idiosyncratic nature, specific assets have little value outside their current use. Such assets may be tangible (computer equipment), intellectual (computer programs), or human. Examples of specific assets include systems development, application maintenance, data warehousing, and highly skilled employees trained to use organization-specific software.

Transaction Cost Economics (TCE) theory is in conflict with the core competency school by suggesting that firms should retain certain specific noncore IT assets in-house. Because of their esoteric nature, specific assets cannot be easily replaced once they are given up in an outsourcing arrangement. Therefore, if the organization should decide to cancel its outsourcing contract with the vendor, it may not be able to return to its pre-outsource state. On the other hand, TCE theory supports the outsourcing of commodity assets, which are easily replaced or obtained from alternative vendors.

Naturally, a CEO's perception of what constitutes a commodity IT asset plays an important role in IT outsourcing decisions. Often, this comes down to a matter of definition and interpretation. For example, most CEOs would define their IT function as a noncore commodity, unless they are in the business of developing and selling IT applications. Consequently, a belief that *all* IT can, and should, be managed by large service organizations tends to prevail. Such misperception reflects, in part, both lack of executive education and the dissemination of faulty information regarding the virtues and limitations of IT outsourcing.[8]

RISKS INHERENT TO IT OUTSOURCING

Large-scale IT outsourcing events are risky endeavors, partly because of the sheer size of these financial deals, and also because of their nature. The level of risk is related to the degree of asset specificity of the outsourced function. The following sections outline some well-documented issues.

Failure to Perform

Once a client firm has outsourced specific IT assets, its performance becomes linked to the vendor's performance. The negative implications of such dependency are illustrated in the financial problems that have plagued the huge outsourcing vendor Electronic Data Systems Corp. (EDS). In a cost-cutting effort, EDS terminated 7000 employees, which impacted its ability to serve other clients. Following an 11-year low in share prices, EDS stockholders filed a class-action

8 This knowledge disconnect is not unique to IT outsourcing; it has been observed by Ramiller and Swanson in their research on how executives respond to what is termed *organizing visions* for IT.

lawsuit against the company. Clearly, vendors experiencing such serious financial and legal problems threaten the viability of their clients also.

Vendor Exploitation of Clients

Large-scale IT outsourcing involves transferring to a vendor "specific assets," such as the design, development, and maintenance of unique business applications that are critical to an organization's survival. Specific assets, while valuable to the client, are of little value to the vendor beyond the immediate contract with the client. Indeed, they may well be valueless should the client organization go out of business. Because the vendor assumes risk by acquiring the assets and can achieve no economies of scale by employing them elsewhere, the client organization will pay a premium to transfer such functions to a third party. Further, once the client firm has divested itself of such specific assets, it becomes dependent on the vendor. The vendor may exploit this dependency by raising service rates to an exorbitant level. As the client's IT needs develop over time beyond the original contract terms, it runs the risk that new or incremental services will be negotiated at a premium. This dependency may threaten the client's long-term flexibility, agility, and competitiveness, and result in even greater vendor dependency.

Outsourcing Costs Exceed Benefits

IT outsourcing has been criticized on the grounds that unexpected costs arise and that the full extent of expected benefits are not realized. One survey revealed that 47 percent of 66 firms surveyed reported that the costs of IT outsourcing exceeded outsourcing benefits. One reason for this is that outsourcing clients often fail to anticipate the costs of vendor selection, contracting, and the transitioning of IT operations to the vendors.

Reduced Security

Information outsourced to offshore IT vendors raises unique and serious questions regarding internal control and the protection of sensitive personal data. When corporate financial systems are developed and hosted overseas, and program code is developed through interfaces with the host company's network, US corporations are at risk of losing control of their information. To a large degree, US firms are reliant on the outsourcing vendor's security measures, data-access policies, and the privacy laws of the host country. For example, a woman in Pakistan obtained patient-sensitive medical data from the University of California Medical Center in San Francisco. She gained access to the data from a medical transcription vendor for whom she worked. The woman threatened to publish the records on the Internet if she did not get a raise in pay. Terrorism in Asia and the Middle East raises additional security concerns for companies outsourcing technology offshore. For example, on March 5, 2005, police in Delhi, India, arrested a cell of suspected terrorists who were planning to attack outsourcing firms in Bangalore, India.

LOSS OF STRATEGIC ADVANTAGE

IT outsourcing may cause incongruence between a firm's IT strategic planning and its business planning functions. Organizations that use IT strategically must align business strategy and IT strategy or run the risk of decreased business performance. To promote such alignment, firms need IT managers and chief information officers (CIOs) who have a strong working knowledge of the organization's business. A survey of 213 IT managers in the financial services industry confirmed that a firm's IT leadership needs to be closely aligned with the firm's competitive strategy. Indeed, some argue that the business competence of CIOs is more important than their IT competence in facilitating strategic congruence.

To accomplish such alignment necessitates a close working relationship between corporate management and IT management in the concurrent development of business and IT strategies. This, however, is difficult to accomplish when IT planning is geographically redeployed offshore or even domestically. Further, because the financial justification for IT outsourcing depends upon

the vendor achieving economies of scale, the vendor is naturally driven toward seeking common solutions that may be used by many clients rather than creating unique solutions for each of them. This fundamental underpinning of IT outsourcing is inconsistent with the client's pursuit of strategic advantage in the marketplace.

AUDIT IMPLICATIONS OF IT OUTSOURCING

Management may outsource its organization's IT functions, but cannot outsource its management responsibilities under SOX for ensuring adequate IT internal controls. The PCAOB specifically states in its Auditing Standard No. 2, that the use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Therefore, if an audit client firm outsources its IT function to a vendor that processes its transactions, hosts key data, or performs other significant services, the auditor will need to conduct an evaluation of the vendor organization's controls, or alternatively obtain an SSAE 16 auditor's report from the vendor organization.

Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is an internationally recognized third-party attestation report designed for service organizations such as IT outsourcing vendors. SSAE 16 was promulgated by the Auditing Standards Board (ASB) of the AICPA and replaced Statement on Auditing Standards No. 70 (SAS 70) on June 15, 2011. Its purpose was to update the outdated SAS 70, which had been in service since 1992. More importantly, its objective was to keep pace with move toward globally accepted international accounting standards.

SSAE 16 is the definitive standard by which client organizations' auditors can determine whether processes and controls at the third-party vendor are adequate to prevent or detect material errors that could impact the client's financial statements. The SSAE 16 report, which is prepared by the service provider's auditor, attests to the functionality of the vendor's system and the adequacy of its internal controls. This is the means by which an outsourcing vendor can obtain a single attest report that may be used by its clients' auditors and thus preclude the need for each client firm auditor to conduct its own audit of the vendor organization's facilities and internal controls.

Figure 15-9 illustrates how an SSAE 16 report works in relation to the vendor, the client firms, and their respective auditors. The outsourcing vendor serves clients 1, 2, 3, and 4 with various IT services. The system processes and internal controls over the outsourced services reside at the vendor location. They are audited by the vendor's auditor, who expresses an opinion and issues an SSAE 16 report. Each of the client firms is audited by different auditors A, B, C, and D, respectively, who as part of their respective audits, rely on the vendor's SSAE 16 report and are thus not compelled to individually test the vendor's controls. Given that a vendor may have hundreds or even thousands of clients, individual testing under SOX would be highly disruptive to the vendor's operations, costly to the client, and impractical.

Service provider auditors issue two types of SSAE 16 reports, Type 1 and Type 2:

The Type 1 report attests to the vendor management's description of their system and the suitability of the design of controls.

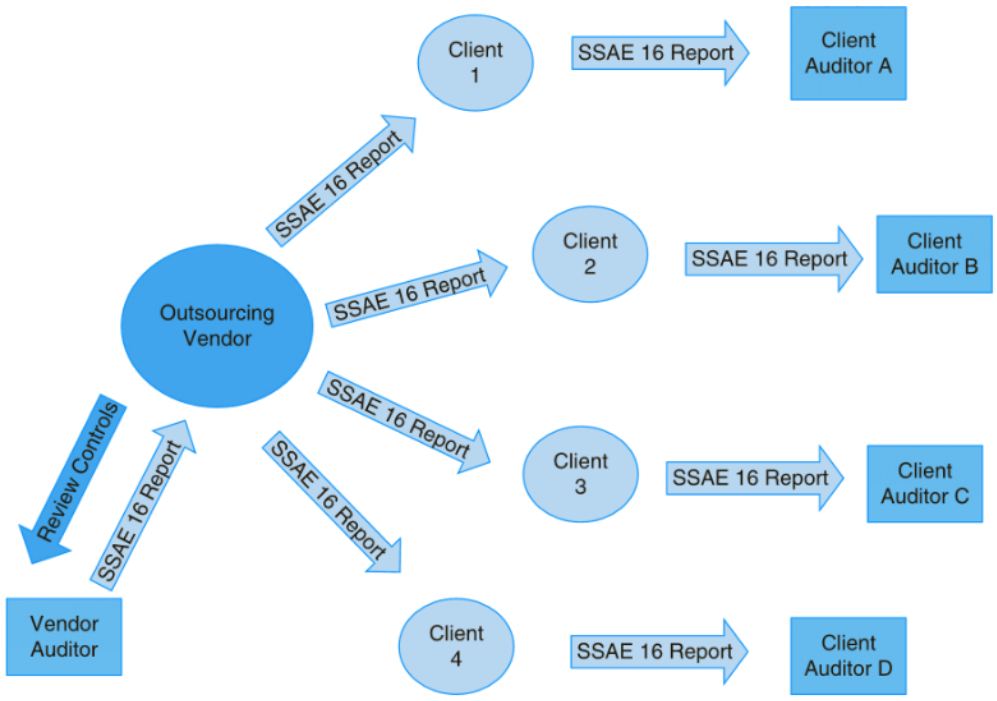
The Type 2 report attests to management's description of their system, the suitability of the design of controls, and the operating effectiveness of controls.

The Type 1 report is the less rigorous of the two and comments only on the suitability of the controls' design. The Type 2 report goes further and assesses whether the controls are operating effectively based on tests conducted by the vendor organization's auditor. Because SOX Section 404 requires the explicit testing of controls, SSAE 16 Type 2 reports are necessary for client firms undergoing a financial statement audit.

SSAE 16 REPORT CONTENTS

The SSAE 16 attest report provides a description of the service provider's system including details of how transactions are processed and results are communicated to their client organizations. The

FIGURE 15-9 SSAE 16 REPORTING



report also describes relevant internal control issues consistent with the COSO control model including the control environment, risk assessment, information and communication systems, control activities and control monitoring. In addition, the report specifies control objectives and the controls designed to achieve those objectives.

In the case of both Type 1 and Type 2 reports, the service provider's auditor will assess whether vendor management used appropriate criteria in evaluating the suitability of the control designs to achieve the control objectives. In the case of Type 2 reports, the auditor will also attest to whether the controls operated effectively throughout the specified period.

Service providers, particularly those in the cloud, may outsource their workload to other service providers. For example, assume Company A, a retailing firm outsources its accounts payable function to Company B who outsources the actual check printing and mailing to Company C. In this situation, Company A is the client firm, Company B is the service provider, and company C is a subservice organization. The importance of company C's system and controls in this relationship is obvious. The SSAE 16 standard was designed to address the subservice organization issue. Two reporting techniques are outlined next.

Carve-out Method: When using the carve-out method, service provider management would exclude the subservice organization's relevant control objectives and related controls from the description of its system. The description would, however, include the nature of the services performed by the subservice organization. Typically the service provider would obtain an SSAE 16 from the subservice organization, and must have controls in place to monitor the effectiveness of the controls at the subservice organization.

Inclusive Method: When using the inclusive method of subservice organization reporting the service provider's description of its system will include the services performed by the subservice organization. In addition, the report will include the relevant control objectives and related controls of the subservice organization.

Summary

This chapter introduced the topic of IT auditing and opened with an overview of auditing in which the key components of an audit were discussed. Topics in this section included auditing standards, the structure of an audit, management assertions, and the audit risk model. Next, the chapter turned to internal control and audit issues related to Sections 302 and 404 of SOX. It began with a review of management and auditor responsibilities under SOX. Then it examined the IT control relationship. This section concluded with a discussion of computer fraud issues. The next section of the chapter presented risks and controls related to IT governance. It began with a brief definition of IT governance and identified its implications for internal control and financial reporting. The structure of the IT function within an organization and the risks that can arise from inappropriate structuring were then discussed. Next, the chapter reviewed computer center threats and controls, which include protecting against damage and destruction from natural disasters, fire, temperature, and humidity. The chapter then presented the key elements of a disaster recovery plan. Several factors need to be considered in such a plan, including providing second-site backup, identifying critical applications, performing backup and off-site storage procedures, creating a disaster recovery team, and testing the DRP. The final section of the chapter examined issues surrounding the growing trend toward IT outsourcing. In particular, it reviewed the theories underlying outsourcing and the expected benefits. IT outsourcing is also associated with significant risks, which were addressed. The chapter concluded with a discussion of audit issues related to outsourcing including the SSAE 16 reporting standard.

Key Terms

access controls (657)
application controls (650)
audit objectives (647)
audit planning (645)
Audit risk (647)
Carve-out Method (673)
Commodity IT assets (670)
computer fraud (652)
computer-aided audit tools and techniques (CAATTs) (646)
control risk (646)
core competency (670)
corporate IT function (660)
Database management fraud (654)
Detection risk (648)
disaster recovery plan (DRP) (665)
distributed data processing (DDP) (658)
eavesdropping (655)
empty shell (666)
Fault tolerance (664)
general computer controls (650)
general controls (650)
Inclusive Method (673)
information technology controls (650)
Inherent risk (648)
IT outsourcing (670)
Management assertions (646)
mirrored data center (666)
off-site storage (665)
Operations fraud (654)
Program fraud (654)
recovery operations center (ROC) (666)
Redundant arrays of independent disks (RAID) (664)
scavenging (655)
Specific IT assets (670)
Statement on Standards for Attestation Engagements No. 16 (SSAE 16) (672)
substantive tests (646)
tests of controls (646)
Transaction Cost Economics (TCE) (670)
Uninterruptible power supplies (664)
user views (656)