Part V

Computer Controls and Auditing

Chapter 15

IT Controls Part I: Sarbanes-Oxley and IT Governance

LEARNING OBJECTIVES

After studying this chapter, you should:

- 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.

This chapter provides an overview of management and auditor responsibilities under Sections 302 and 404 of the Sarbanes-Oxley Act (SOX). The design, implementation, and assessment of internal control over the financial reporting process form the central theme of these sections. Our study of internal control follows the Committee of Sponsoring Organizations of the Treadway Commission (COSO) control framework. Under COSO, information technology (IT) internal controls are divided into application controls and general controls. Because of the extensive nature of the material and its importance to accountants, this and the remaining two chapters are devoted to the subject. This chapter presents controls and tests of controls related to IT governance, including organizing the IT function, controlling computer center operations, and designing an adequate disaster recovery plan. Chapter 16 deals with the security and access controls over operating systems, databases, and networks. Chapter 17 addresses systems development, program changes, and application control issues. As background material, the appendix to this chapter contains a brief overview of auditing concepts and principles.

Overview of Sections 302 and 404 of SOX

SOX of 2002 established new corporate governance regulations and standards for public companies registered with the Securities and Exchange Commission (SEC). While 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 CEO) to certify financial and other information contained in the organization's quarterly and annual reports. The rule also requires them to certify the internal controls over financial reporting. The certifying officers are required to have designed internal controls, or 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. a statement of management's responsibility for establishing and maintaining adequate internal control
2. an assessment of the effectiveness of the company's internal controls over financial reporting
3. a statement that the organization's external auditor has issued an attestation report on the company's internal controls
4. an explicit written conclusion as to the effectiveness of internal control over financial reporting[1]
5. a statement identifying the framework used by management to conduct their assessment of internal controls.

Regarding the final point, the SEC has made specific reference to COSO as a recommended control framework. Furthermore, the PCAOB's 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.[2] We discussed the key elements of the COSO framework, which is the basis for SAS 78, in Chapter 3. Our focus at this point is on IT controls (a subset of control activities), which were not previously discussed. This aspect of the COSO framework is used to present control and audit issues in this and the following two chapters.

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. COSO identifies two broad groupings of information

1 Management may not conclude that internal controls are effective if one or more material weaknesses exist. In addition, management must disclose all material weaknesses that exist as of the end of the most recent fiscal year.

2 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.

system controls: application controls and general controls. The objectives of **application controls** are to 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 account receivable check digits 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. Application controls are examined in detail in Chapter 17.

The second broad group of controls that COSO identifies is **general controls.** They 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, security and access to **operating systems** and databases, application acquisition and development, and program changes.

Whereas 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. An individual who is able to circumvent database security (either directly or via a malicious program), may then change, steal, or corrupt stored transaction data. Thus, general controls are needed to support the functioning of application controls, and both are needed to ensure accurate financial reporting.

Audit Implications of Sections 302 and 404

The material covered in the remainder of this chapter and the following chapters assumes a basic understanding of the audit process. Specifically, the reader should:

1. Be able to distinguish between the attest function and assurance.
2. Understand the concept of management assertions and recognize the relationship between assertions and audit objectives.
3. Know the difference between tests of controls and substantive tests and understand the relationship between them.

The appendix to this chapter contains a brief overview of these topics. Those lacking this knowledge should review the appendix before continuing with this section.

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 management's assessment 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 new audit opinion is high. Indeed, the auditor is precluded from issuing an unqualified opinion if only one material weakness in internal control is detected. Interestingly, auditors are permitted to simultaneously render a qualified opinion

on management's assessment of internal controls and an unqualified opinion on the financial statements. In other words, it is technically possible for auditors to find internal controls over financial reporting to be weak, but conclude through substantive tests that the weaknesses did not cause the financial statements to be materially misrepresented.

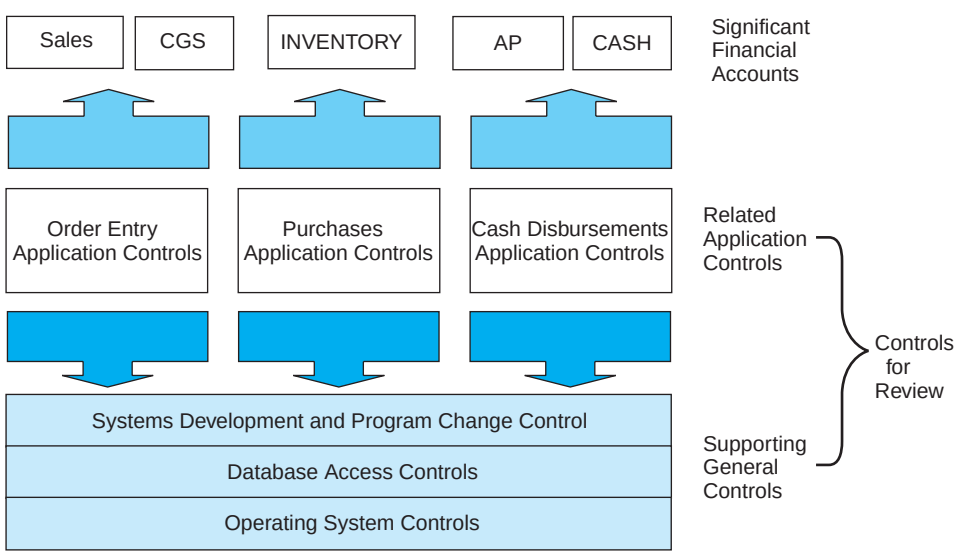
As part of the new attestation responsibility, the PCAOB's Standard No. 5 specifically requires auditors to understand transaction flows, including the controls pertaining to how transactions are initiated, authorized, recorded, and reported. This involves first selecting the financial accounts that have material implications for financial reporting. Then, auditors need to identify the application controls related to those accounts. As previously noted, the reliability of these application controls rests on the IT general controls that support them, such as controls over access to databases, operating systems and networks, and so on. The sum of these controls, both application and general, constitute the relevant internal controls over financial reporting that need to be reviewed. Figure 15-1 illustrates this IT control relationship.

Compliance with Section 404 requires management to provide the external auditors with documented test results of functioning controls as supporting evidence for assertions in its report on control effectiveness. The organization's internal audit function or a specialized SOX group would likely perform these tests. Hence, management must actually perform its own tests of controls prior to the auditors performing theirs.

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.

FIGURE 15-1 IT Control Relationship



- 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 expressly required to test them.

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 a risk-based approach rather than a one-size-fits-all approach to the design and assessment of controls is inappropriate. 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 text 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. Though 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 on 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.

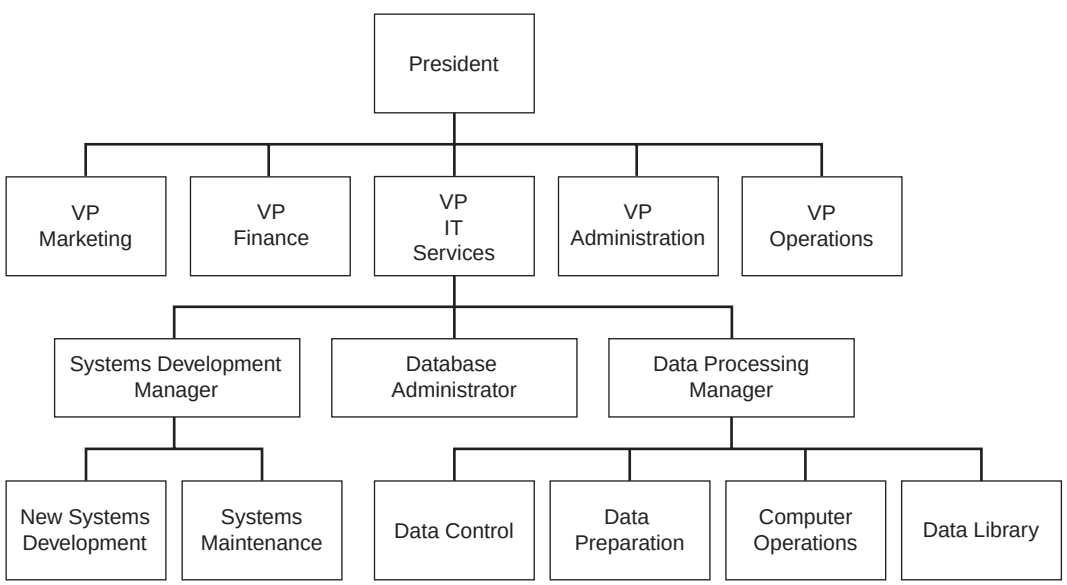
Segregation of Duties within the Centralized Firm

Figure 15-2 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 the greatest 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 execution. Such changes may be temporary (on the fly) and will disappear with little or no trace when the application terminates.

FIGURE 15-2 **Organizational Chart of a Centralized IT Function**



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 15-2 shows how the DBA function is organizationally independent.

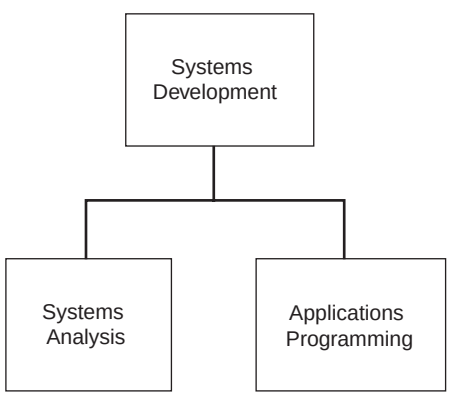
Separating the DBA from Systems Development. Programmers create applications that access, update, and retrieve data from the database. Chapter 9 illustrated how database access control is achieved through the creation of user views, which is a DBA responsibility. To achieve database access, therefore, 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 15-3. 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 (SDLC). 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.

FIGURE 15-3 Alternative Organization of Systems Development



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 also has 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, 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 15-2 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 in 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 such as source program library controls discussed in Chapter 17. Whereas organizational separations alone cannot guarantee that computer frauds will not occur, they are critical to creating the necessary control environment.

The Distributed Model

Chapter 1 examined the impact on organizational structure of moving to a distributed data processing (DDP) model in which end-user departments control IT services. The effect of this is to consolidate some computer functions that are traditionally separated and to distribute some activities that are consolidated under the centralized model. In spite of the many advantages DDP provides, the approach carries IT control implications that management and accountants should recognize. These are discussed in the following sections.

Incompatibility

Distributing responsibility for the purchases of software and hardware can result in uncoordinated and poorly conceived decisions. Organizational users, working independently, may select different and incompatible operating systems, technology platforms, spreadsheets, word processing, and database packages, which can impair internal communications.

Redundancy

Autonomous systems development activities throughout the firm can result in the creation of redundant applications and databases. Programs that one user creates that 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 reproduced, resulting in a high level of data redundancy.

Consolidating Incompatible Activities

The redistribution of IT functions to user areas can result in the creation of many very small units. Achieving an adequate segregation of duties may be economically or operationally infeasible in this setting. Thus, one person (or a small group) may be responsible for program development, program maintenance, and computer operations.

Acquiring Qualified Professionals

End users are typically not qualified to evaluate the technical credentials and relevant experience of prospective IT employees. Also, because the organizational unit into which these candidates are entering is small, opportunities for personal growth, continuing education, and promotion are limited. For these reasons, distributed IT units may have difficulty attracting highly qualified personnel.

Lack of Standards

For the aforementioned reasons, standards for systems development, documentation, and evaluating performance tend to be unevenly applied or nonexistent in the distributed environment.

Creating a Corporate IT Function

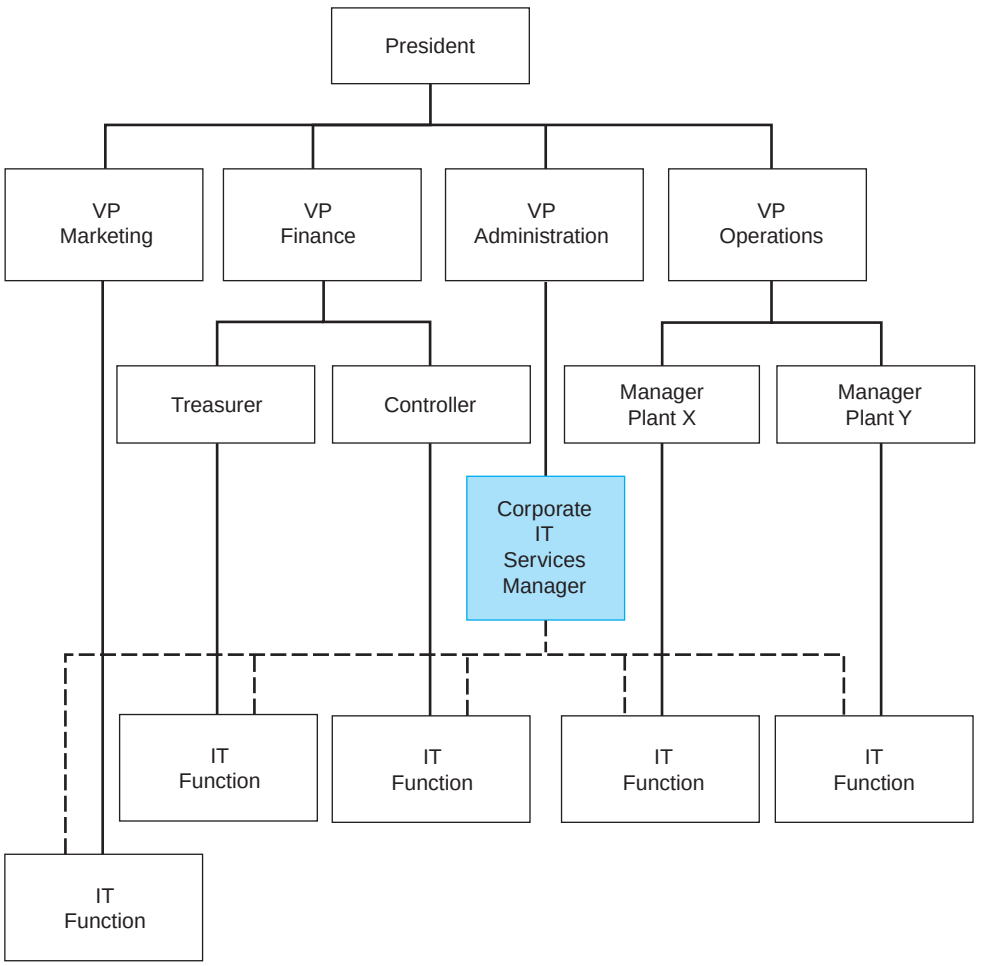
The completely centralized and the fully distributed models represent extreme positions on a continuum of structural alternatives. The needs of most firms fall somewhere between these end points. For these firms, the control problems associated with DDP can, to some extent, be overcome by implementing a **corporate IT function**. Figure 15-4 illustrates this organizational approach.

The corporate IT function is a leaner unit with a different mission than that of the centralized IT function shown in Figure 15-4. This group provides technical advice and expertise to the various distributed IT functions, as the dotted lines represent in Figure 15-4. 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.

FIGURE 15-4 **Distributed Organization with Corporate IT Function**



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 verify that individuals in incompatible areas are segregated in accordance with the level of potential risk and in a manner that promotes a working environment. This is an environment in which formal, rather than casual, relationships need to exist between incompatible tasks.

Audit Procedures Relating to Organizational Structure

The following tests of controls would enable the auditor to achieve the control objectives.

- 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 rights and privileges 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 the 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, though 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.

a. Automatic and manual alarms should be placed in strategic locations around the installation. These alarms should be connected to a permanently staffed firefighting station.
b. 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.

c. There should be manual fire extinguishers placed at strategic locations.
d. The building should be of sound construction to withstand water damage that fire suppression equipment causes.
e. 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 auditor's objective is to evaluate the controls governing computer center security. Specifically, the auditor must verify that (1) physical security controls are adequate to reasonably protect the organization from physical exposures; (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 routine operations as well as system failures.

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 that each 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 where 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 the company's needs priority. 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 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. For example, 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. 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 predisaster business activity levels. Immediate recovery efforts, however, should focus on restoring those applications and data that are critical to the organization's short-run 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 the 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 CASE documentation tools.

Backup Supplies and Source Documents

The firm should maintain backup inventories of supplies and source documents used in the 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.

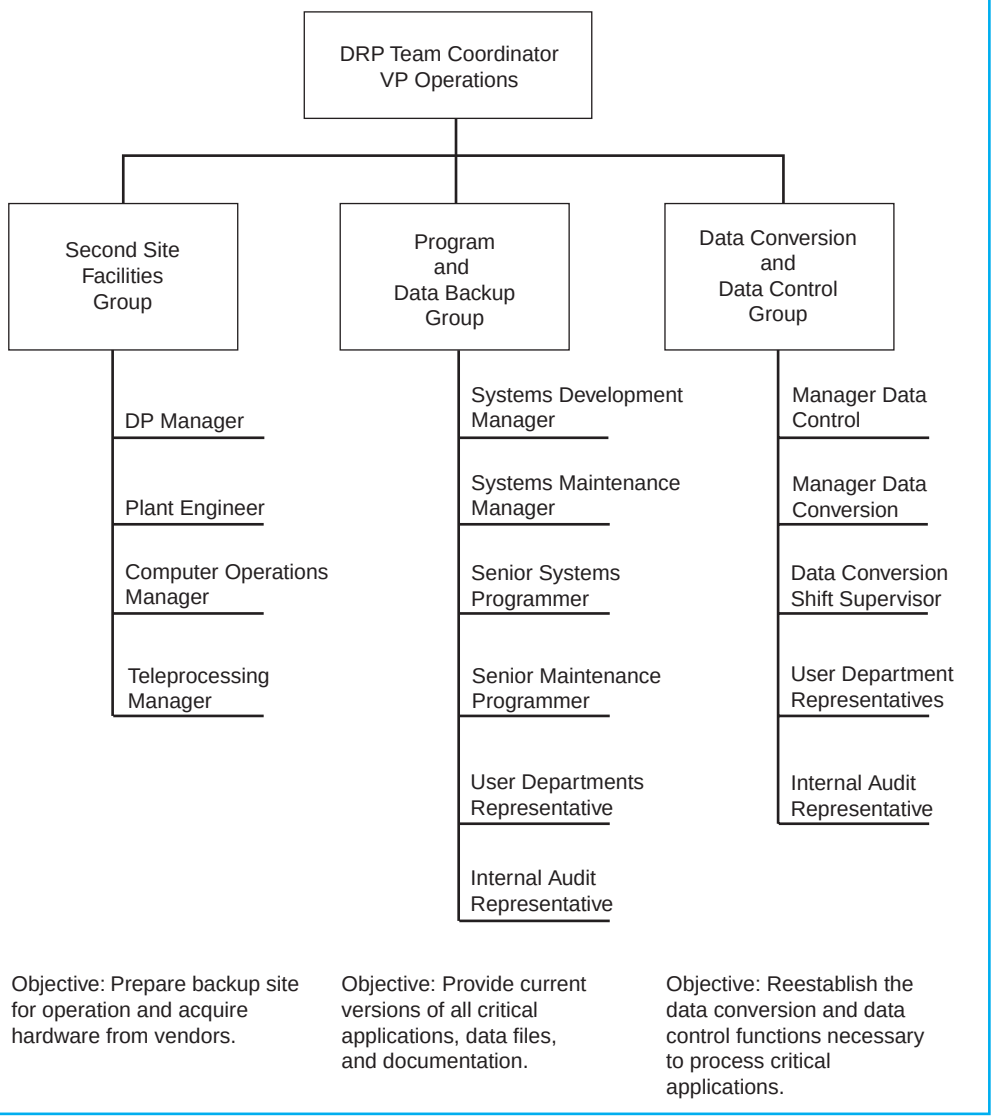
Figure 15-5 presents an organizational chart depicting the possible composition of a disaster recovery team. The team members should be experts in their areas and have assigned tasks. Following a disaster, team members will delegate subtasks to their subordinates. It should be noted that traditional 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.

Testing the DRP

The most neglected aspect of contingency planning is testing 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.

FIGURE 15-5 **Disaster Recovery Team**



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 current 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 determine 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.

Summary

This chapter examined some of the internal control issues and audit issues that have arisen out of Sections 302 and 404 of SOX. It began with a review of management and auditor responsibilities under SOX. Then we examined the COSO control framework that the PCAOB and the SEC recommend. Next, the chapter presented exposures that arise in connection with organizational structure. In these general areas, exposures are controlled through important segregation of incompatible duties. The chapter reviewed computer center threats. To ensure the physical security of its computer equipment, a firm must choose a location that is not susceptible to human-made or natural hazards. The building that houses the computer equipment must be soundly and strategically constructed and equipped with systems that regulate air filtration, temperature, and humidity. An adequate fire suppression system is also required, because fire is the most common threat to the computer center. Finally, the chapter 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.

Appendix

Recent developments in IT have had a tremendous impact on the field of auditing. In this text, we have seen how IT has inspired the reengineering of traditional business processes to promote more efficient operations and to improve communications within the entity and between the entity and its customers and suppliers. These advances, however, have introduced new risks that require unique internal controls. They have engendered the need for new techniques for evaluating controls and for ensuring the security and accuracy of corporate data and the information systems that produce it. This appendix presents an overview of alternative audit approaches and presents the general structure of an audit.

Attest Services versus Assurance Services

An important starting point for this body of material is to draw a distinction between the auditor's traditional attestation function and assurance services. The attest service is defined as

> an engagement in which a practitioner is engaged to issue, or does issue, a written communication that expresses a conclusion about the reliability of a written assertion that is the responsibility of another party (SSAE No. 1, AT Section 100.01).

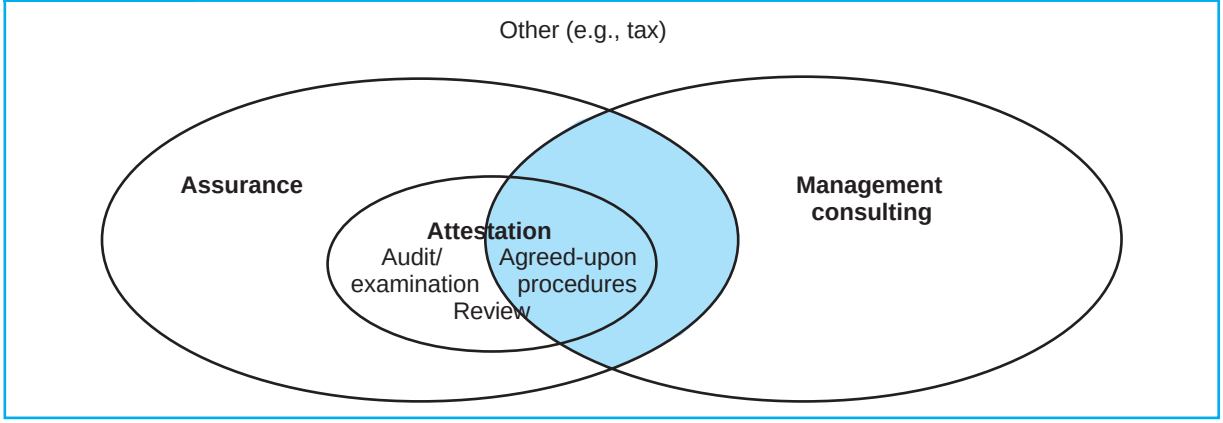
The following requirements apply to attestation services:

- Attestation services require written assertions and a practitioner's written report.
- Attestation services require the formal establishment of measurement criteria or their description in the presentation.
- The levels of service in attestation engagements are limited to examination, review, and application of agreed-upon procedures.

Assurance services constitute a broader concept that encompasses, but is not limited to, attestation. The relationship between these services is illustrated in Figure 15-6.

Assurance services (or advisory services) are professional services designed to improve the quality of information, both financial and nonfinancial, that decision makers use. The domain of assurance services is intentionally unbounded so that it does not inhibit the growth of future services that are currently unforeseen. For example, assurance services may be contracted to provide information about the quality

FIGURE 15-6 **Relationship between Assurance Services and Attest Services**



Source: Based on the AICPA *Special Committee Report on Assurance Services*.

or marketability of a product. Alternatively, a client may need information about the efficiency of a production process or the effectiveness of its network security system. Assurance services are intended to help clients make better decisions by improving information.

Prior to the passage of SOX, accounting firms could provide assurance services concurrently to audit (attest function) clients. SOX legislation, however, greatly restricts the types of nonaudit services that auditors may render audit clients. It is now unlawful for a registered public accounting firm that is currently providing attest services for a client to provide the following services:

- bookkeeping or other services related to the accounting records or financial statements of the audit client
- financial information systems design and implementation
- appraisal or valuation services, fairness opinions, or contribution-in-kind reports
- actuarial services
- internal audit outsourcing services
- management functions or human resources
- broker or dealer, investment adviser, or investment banking services
- legal services and expert services unrelated to the audit
- any other service that the Board determines, by regulation, is impermissible

The organizational units responsible for providing IT-related services and support usually have the words risk management in their title, such as: IT Risk Management, Information Systems Risk Management, or Global Risk Management. These units are typically a division of assurance services whose members work with the financial audit staff to perform IT related tasks as part of the attestation function. In addition, they provide IT advisory services to nonaudit clients.

The material outlined in this appendix relates to tasks that risk management professionals normally conduct during an IT audit. In the pages that follow, we examine what constitutes an audit and how audits are structured. Keep in mind, however, that in many cases the purpose of the audit task, rather than the task itself, defines the service being rendered. Therefore, the issues and procedures described in this appendix apply to the broader context of assurance services, which include, but are not limited to, attest services. They also relate directly to the internal audit function.

What Is an External Financial Audit?

An external financial audit is an attestation performed by an expert—the auditor—who expresses an opinion regarding the presentation of financial statements. The audit objective is associated with the presentation of financial statements, in particular that in all material respects, the statements are fairly presented. The external auditor is an independent auditor and is a certified public accountant (CPA). The SEC requires all publicly traded companies to be subject annually to a financial audit by an independent auditor. CPAs represent the interests of outsiders: stockholders, creditors, government agencies, and the public. Public confidence in the reliability of the company's internally produced financial statements rests directly on the statements that an independent auditor evaluates.

The external auditor must follow strict rules in conducting financial audits. These authoritative rules have been defined by federal law (Sarbanes-Oxley Act, 2002), the SEC, the Financial Accounting Standards Board (FASB), and the American Institute of Certified Public Accountants (AICPA). Until recently, the SEC has delegated most of that authority to the AICPA and FASB, the majority of whose members are CPAs. SOX established the Public Company Accounting Oversight Board (PCAOB) to oversee much of the guidelines and standards of financial auditing, which potentially could replace the function served by FASB, and some of the functions the AICPA, including reprimands and penalties for CPAs who are convicted of certain crimes or guilty of certain infractions.

The public expression of the auditor's opinion is the culmination of a systematic audit process that involves three conceptual phases: (1) familiarization with the organization's business, (2) evaluating and

testing internal controls, and (3) assessing the reliability of financial data. The specific elements of the audit process are examined later in this appendix.

Auditing Standards

The product of the attestation function is a formal written report that expresses an opinion about the reliability of the assertions contained in the financial statements. The auditor's report expresses an opinion as to whether the financial statements are in conformity with generally accepted accounting principles. 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 ten generally accepted auditing standards (GAAS) presented in Table 15-1.

Auditing standards are divided into three classes: general qualification standards, fieldwork standards, and reporting standards. GAAS establishes a framework for prescribing auditor performance, but 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. SASs are often referred to as auditing standards, or GAAS, although they are not the ten generally accepted auditing standards.

Statements on Auditing Standards

The AICPA issued the first SAS (SAS 1) 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 SAS falls on the individual auditor.

TABLE 15-1 Generally Accepted Auditing Standards

General Standards	Standards of Fieldwork	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.

External Auditing versus Internal Auditing

External auditing is often called independent auditing because it is done by certified public accountants who are independent of the organization being audited. External auditors represent the interests of third-party stakeholders in the organization, such as stockholders, creditors, and government agencies. Because the focus of the external audit is on the financial statements, this type of audit is called a financial audit.

The Institute of Internal Auditors defines internal auditing as an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization.[3] Internal auditors perform a wide range of activities on behalf of the organization, including conducting financial audits, examining an operation's compliance with organizational policies, reviewing the organization's compliance with legal obligations, evaluating operational efficiency, detecting and pursuing fraud within the firm, and conducting IT audits.

The characteristic that conceptually distinguishes internal auditors from external auditors is their respective constituencies: external auditors represent outsiders, and internal auditors represent the interests of the organization. Nevertheless, in this capacity, internal auditors often cooperate with and assist external auditors in performing financial audits. This is done to achieve audit efficiency and reduce audit fees. For example, a team of internal auditors can perform tests of computer controls under the supervision of a single external auditor.

The independence and competence of the internal audit staff determine the extent to which external auditors may cooperate with and rely on work that internal auditors perform. Some internal audit departments report directly to the controller. Under this arrangement, the internal auditor's independence is compromised, and the professional standards prohibit the external auditor from relying on evidence that the internal auditors provide. In contrast, external auditors can rely in part on evidence gathered by internal audit departments that are organizationally independent and that report to the board of directors' audit committee. A truly independent internal audit staff adds value to the audit process. Internal auditors can gather audit evidence throughout a fiscal period; external auditors can then use this evidence at year-end to conduct more efficient, less disruptive, and less costly audits of the organization's financial statements.

What Is an IT Audit?

An IT audit focuses on the computer-based aspects of an organization's information system. This includes assessing the proper implementation, operation, and control of computer resources. Because most modern information systems employ information technology, the IT audit is typically a significant component of all external (financial) and internal audits.

The Elements of Auditing

To this point, we have painted a broad picture of auditing. Let's now fill in some details. The following definition of auditing is applicable to external auditing, internal auditing, and IT auditing:

> Auditing is a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users.[4]

This seemingly obtuse definition contains several important points that are examined in the following sections.

---

3 Institute of Internal Auditors, Standards of Professional Practice of Internal Auditing (Orlando, FL: Institute of Internal Auditors, 1978).

4 AAA Committee on Basic Auditing Concepts, "A Statement of Basic Auditing Concepts," *Accounting Review*, supplement to vol. 47, 1972.

A Systematic Process. Conducting an audit is a systematic and logical process that applies to all forms of information systems. Though important in all audit settings, a systematic approach is particularly important in the IT environment. The lack of physical procedures that can be visually verified and evaluated injects a high degree of complexity into the IT audit. Therefore, a logical framework for conducting an audit in the IT environment is critical to help the auditor identify important processes and data files.

Management Assertions and Audit Objectives. The organization's financial statements reflect a set of management assertions about the financial health of the entity. The task of the auditor is to determine whether the financial statements are fairly presented. To accomplish this, the auditor establishes audit objectives, designs procedures, and gathers evidence that corroborates or refutes management's assertions. These assertions fall into five general categories:

1. The existence or occurrence assertion affirms that all assets and equities contained in the balance sheet exist and that all transactions in the income statement actually occurred.
2. The completeness assertion declares that no material assets, equities, or transactions have been omitted from the financial statements.
3. The rights and obligations assertion maintains that the entity owns assets appearing on the balance sheet and that the liabilities reported are obligations.
4. The valuation or allocation assertion states that assets and equities are valued in accordance with generally accepted accounting principles and that allocated amounts such as depreciation expense are calculated on a systematic and rational basis.
5. The presentation and disclosure assertion alleges that financial statement items are correctly classified (for example, long-term liabilities will not mature within one year) and that footnote disclosures are adequate to avoid misleading the users of financial statements.

Generally, auditors develop their audit objectives and design audit procedures based on the preceding assertions. The example in Table 15-2 outlines these procedures.

Obtaining Evidence. Auditors seek evidential matter that corroborates management assertions. In the IT environment, this involves gathering evidence relating to the reliability of computer controls as well as the contents of databases that computer programs have processed. Evidence is collected by performing tests of controls, which establish whether internal controls are functioning properly, and substantive tests, which determine whether accounting databases fairly reflect the organization's transactions and account balances.

Ascertaining the Degree of Correspondence with Established Criteria. The auditor must determine whether weaknesses in internal controls and misstatements found in transactions and account balances are material. In all audit environments, assessing materiality is an auditor judgment. In an IT environment, however, technology and a sophisticated internal control structure further complicate this decision.

Communicating Results. Auditors must communicate the results of their tests to interested users. Independent auditors render a report to the audit committee of the board of directors or stockholders of a company. The audit report contains, among other things, an audit opinion. This opinion is distributed along with the financial report to interested parties both internal and external to the organization. IT auditors often communicate their findings to internal and external auditors, who can then integrate these findings with the non-IT aspects of the audit.

The Structure of an IT Audit

The IT audit is generally divided into three phases: audit planning, tests of controls, and substantive testing. Figure 15-7 illustrates the steps involved in these phases.

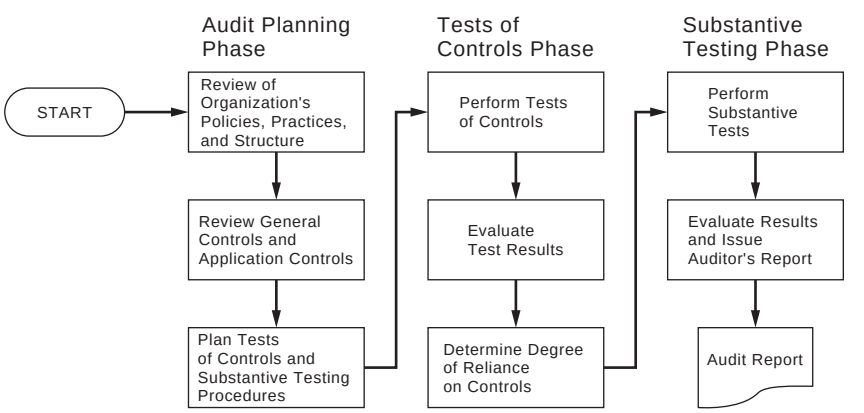
TABLE 15-2 Audit Objectives and Audit Procedures Based on Management Assertions

Management Assertion	Audit Objective	Audit Procedure
Existence or Occurrence	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 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.
Presentation and Disclosure	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 Planning

The first step in the IT audit is audit planning. Before the auditor can determine the nature and extent of the tests to perform, he or she must gain a thorough understanding of the client's business. A major part of this phase of the audit is the analysis of audit risk (discussed later). The objective of the auditor is to obtain sufficient information about the firm to plan the other phases of the audit. The risk analysis incorporates an overview of the organization's internal controls. During the review of controls, the auditor attempts to understand the organization's policies, practices, and structure. In this phase of the audit, the

FIGURE 15-7 Phases of an IT Audit



auditor also identifies the financially significant applications and attempts to understand the controls over the primary transactions that these applications process.

The techniques for gathering evidence at this phase include questionnaires, interviewing management, reviewing systems documentation, and observing activities. During this process, the IT auditor must identify the principal exposures and the controls that attempt to reduce these exposures. Having done so, the auditor proceeds to the next phase, where he or she 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. To accomplish this, the auditor performs various tests of controls. The evidence-gathering techniques used in this phase may include both manual techniques and specialized computer audit techniques.

At the conclusion of the tests of controls phase, the auditor must assess the quality of the internal controls. The degree of reliance the auditor can ascribe to internal controls affects the nature and extent of substantive testing. The relationship between tests of controls and substantive tests is discussed later.

Substantive Testing

The third phase of the audit process focuses on financial data. This 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 sometimes used to verify account balances. The auditor selects a sample of accounts receivable balances and traces these back to their source—the customers—to determine if in fact a bona fide customer owes the amount stated. By so doing, the auditor can verify the accuracy of each account in the sample. Based on such sample findings, the auditor is able to draw conclusions about the fair value of the entire accounts receivable asset.

Some substantive tests are physical, labor-intensive activities such as counting cash, counting inventories in the warehouse, and verifying the existence of stock certificates in a safe. In an IT environment, the information needed to perform substantive tests (such as account balances and names and addresses of individual customers) is contained in data files that often must be extracted using computer-assisted audit tools and techniques (CAATTs) software.

Assessing Audit Risk and Designing Tests of Controls

Audit risk is the probability that the auditor will render an unqualified (clean) opinion on financial statements that are, in fact, materially misstated. Errors may cause material misstatements, or irregularities, or both. Errors are unintentional mistakes. Irregularities are intentional misrepresentations to perpetrate a fraud or to mislead the users of financial statements. The auditor's objective is to minimize audit risk by performing tests of controls and substantive tests.

Audit Risk Components

The three components of audit risk are inherent risk, control risk, and detection risk.

Inherent Risk

Inherent risk is associated with the unique characteristics of the business or industry of the client.[5] Firms in declining industries have greater inherent risk than firms in stable or thriving industries. Auditors cannot

5 Auditing Standards Board, AICPA Professional Standards (New York: AICPA, 1994) AU Section 312.20.

reduce the level of inherent risk. Even in a system where excellent controls protect financial data, financial statements can be materially misstated.

To illustrate inherent risk, assume that the audit client's financial statements show an accounts receivable balance of $10 million. Unknown to the auditor and the client, several customers with accounts receivable totaling $2 million are about to go out of business. These accounts, which are a material component of the total accounts receivable balance of $10 million, are not likely to be collected. To represent these accounts as an asset in the financial statements would be a material misstatement of the firm's economic position.

Control Risk

Control risk is the likelihood that the control structure is flawed because controls are either absent or inadequate to prevent or detect errors in the accounts.[6] To illustrate control risk, consider the following partial customer sales record, which the sales order system processes.

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

Assuming the Quantity and Unit Price fields in the record are correctly presented, then the extended amount (Total) value of $2,000 is in error. An 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 reduce 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 the application processes 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 is the risk that auditors are willing to accept that errors not detected or prevented by the control structure will also not be detected by the auditor.[7] Auditors set an acceptable level of detection risk (called planned detection risk) that influences the level of substantive tests that they perform. For example, more substantive testing would be required when the planned detection risk is 1 percent than when it is 5 percent.

The Relationship between Tests of Controls and Substantive Tests

Tests of controls and substantive tests are auditing techniques used for reducing total audit risk. The relationship between tests of controls and substantive tests varies according to the auditor's risk assessment of the organization. The stronger the internal control structure, the lower the control risk and the less substantive testing the auditor must do. This is because the likelihood of errors in the accounting records is reduced. In other words, when controls are strong, the auditor may limit substantive testing. However, 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 forces the auditor to extend substantive testing to search for misstatements in financial data that control errors as well as business problems inherent to the organization cause. Because substantive tests are labor-intensive and time-consuming, they are expensive. Increased substantive testing translates into longer and more disruptive audits and higher audit costs.

---

6 Ibid.
7 Ibid.

Key Terms

access controls (730)
application controls (726)
corporate IT function (732)
disaster recovery plan (DRP) (738)
empty shell (738)
fault tolerance (736)
general computer controls (726)
general controls (726)
information technology controls (726)
mirrored data center (739)
off-site storage (738)
operating systems (726)
recovery operations center (ROC) (738)
redundant arrays of independent disks (RAID) (736)
uninterruptible power supplies (736)
user views (730)

Review Questions

1. SOX contains many sections. Which sections are the focus of this chapter?
2. What control framework does the PCAOB recommend?
3. COSO identifies two broad groupings of information system controls. What are they?
4. What are the objectives of application controls?
5. Give three examples of application controls.
6. Define general controls.
7. How do automated authorization procedures differ from manual authorization procedures?
8. Explain why certain duties that are deemed incompatible in a manual system may be combined in a CBIS environment. Give an example.
9. What are the three primary CBIS functions that must be separated?
10. What exposures do data consolidation in a CBIS environment pose?
11. Differentiate between general and application controls. Give two examples of each.
12. What are the primary reasons for separating operational tasks?
13. What problems may occur as a result of combining applications programming and maintenance tasks into one position?
14. Why is poor-quality systems documentation a prevalent problem?
15. What is the role of a corporate computer services department? How does this differ from other configurations?
16. What are the five control implications of distributed data processing?
17. List the control features that directly contribute to the security of the computer center environment.
18. What is fault tolerance?
19. What is RAID?
20. What is the purpose of an audit?
21. Discuss the concept of independence within the context of an audit.
22. What is the meaning of the term *attest services*?
23. What are assurance services?
24. What are the conceptual phases of an audit? How do they differ between general auditing and IT auditing?
25. Distinguish between internal and external auditors.
26. What are the four primary elements described in the definition of auditing?
27. Explain the concept of materiality.
28. What tasks do auditors perform during audit planning, and what techniques are used?
29. Distinguish between tests of controls and substantive testing.
30. What is audit risk?
31. Distinguish between errors and irregularities. Which do you think concern auditors the most?
32. Distinguish between inherent risk and control risk. How do internal controls affect inherent risk and control risk, if at all? What is the role of detection risk?
33. What is the relationship between tests of controls and substantive tests?
34. List four general control areas.
35. What types of documents would an auditor review in testing organizational structure controls? Why is it also important to observe actual behavior?
36. What are some tests of physical security controls?

Discussion Questions

1. Discuss the key features of Section 302 of SOX.
2. Discuss the key features of Section 404 of SOX.
3. Section 404 requires management to make a statement identifying the control framework used to conduct their assessment of internal controls. Discuss the options in selecting a control framework.
4. Explain how general controls impact transaction integrity and the financial reporting process.
5. Prior to SOX, external auditors were required to be familiar with the client organization's internal controls, but not test them. Explain.
6. Does a qualified opinion on management's assessment of internal controls over the financial reporting system necessitate a qualified opinion on the financial statements? Explain.
7. The PCAOB's Standard No. 5 specifically requires auditors to understand transaction flows in designing their tests of controls. What steps does this entail?
8. What fraud detection responsibilities (if any) does SOX impose on auditors?
9. A bank in California has 13 branches spread throughout northern California, each with its own minicomputer where its data are stored. Another bank has 10 branches spread throughout California, with the data being stored on a mainframe in San Francisco. Which system do you think is more vulnerable to unauthorized access? Excessive losses from disaster?
10. Compare and contrast the following disaster recovery options: empty shell, recovery operations center, and internally provided backup. Rank them from most risky to least risky, as well as from most costly to least costly.
11. Who should determine and prioritize the critical applications? How is this done? How frequently is it done?
12. Discuss the differences between the attest function and assurance services.
13. Define the management assertions of existence or occurrence, completeness, rights and obligations, valuation or allocation, and presentation and disclosure.
14. An organization's internal audit department is usually considered an effective control mechanism for evaluating the organization's internal control structure. Birch Company's internal auditing function reports directly to the controller. Comment on the effectiveness of this organizational structure.
15. Discuss why any distinction between IS auditing and financial auditing is not meaningful.
16. Discuss how the process of obtaining audit evidence in a CBIS is inherently different than in a manual system.
17. Some internal controls can be tested objectively. Discuss some internal controls that you think are relatively more subjective to assess in terms of adequacy than others.
18. Give a specific example, other than the one in the chapter, to illustrate the relationship between exposure, control, audit objective, and tests of control.
19. Discuss the subjective nature of auditing computer center security.

Multiple-Choice Questions

1. Which of the following is NOT a requirement in management's report on the effectiveness of internal controls over financial reporting?
   a. A statement of management's responsibility for establishing and maintaining adequate internal control user satisfaction.
   b. A statement that the organization's internal auditors have issued an attestation report on management's assessment of the company's internal controls.
   c. A statement identifying the framework management uses to conduct its assessment of internal controls.
   d. An explicit written conclusion as to the effectiveness of internal control over financial reporting.

2. Which of the following is NOT an implication of Section 302 of SOX?
   a. Auditors must determine whether changes in internal control have, or are likely to, materially affect internal control over financial reporting.
   b. Auditors must interview management regarding significant changes in the design or operation of internal control that occurred since the last audit.
   c. Corporate management (including the CEO) must certify monthly and annually their organization's internal controls over financial reporting.
   d. Management must disclose any material changes in the company's internal controls that have occurred during the most recent fiscal quarter.
3. Which of the following statements is true?
   a. Both the SEC and the PCAOB require the use of the COSO framework.
   b. Both the SEC and the PCAOB require the COBIT framework.
   c. The SEC recommends COBIT, and the PCAOB recommends COSO.
   d. Any framework can be used that encompass all of COSO's general themes.
   e. Both c and d are true.
4. Which of the following is NOT a control implication of distributed data processing?
   a. redundancy
   b. user satisfaction
   c. incompatibility
   d. lack of standards
5. Which of the following disaster recovery techniques may be least optimal in the case of a widespread natural disaster?
   a. empty shell
   b. ROC
   c. internally provided backup
   d. they are all equally beneficial
6. Which of the following is NOT a potential threat to computer hardware and peripherals?
   a. low humidity
   b. high humidity
   c. carbon dioxide fire extinguishers
   d. water sprinkler fire extinguishers
7. Computer accounting control procedures are referred to as general or application controls. The primary objective of application controls in a computer environment is to
   a. ensure that the computer system operates efficiently.
   b. ensure the validity, completeness, and accuracy of financial transactions.
   c. provide controls over the electronic functioning of the hardware.
   d. plan for the protection of the facilities and backup for the systems.
8. Which of the following is NOT a task performed in the audit planning phase?
   a. reviewing an organization's policies and practices
   b. determining the degree of reliance on controls
   c. reviewing general controls
   d. planning substantive testing procedures
9. Which of the following risks does the auditor least control?
   a. inherent risk
   b. control risk
   c. detection risk
   d. all are equally controllable
10. Which of the following would strengthen organizational control over a large-scale data processing center?
   a. requiring the user departments to specify the general control standards necessary for processing transactions.
   b. requiring that requests and instructions for data processing services be submitted directly to the computer operator in the data center.
   c. having the database administrator report to the manager of computer operations.
   d. assigning maintenance responsibility to the original system designer who best knows its logic.
   e. none of the above.

Problems

1. Physical Security

Avatar Financials, Inc., located on Madison Avenue, New York, is a company that provides financial advice to individuals and small to mid-sized businesses. Its primary operations are in wealth management and financial advice. Each client has an account where basic personal information is stored on a server within the main office in New York City. The company also keeps the information about the amount of investment of each client on a separate server at their data center in Bethlehem, Pennsylvania. This information includes the total value of the portfolio, type of investments made, the income structure of each client, and associated tax liabilities.

In the last few years, larger commercial banks have started providing such services and are competing for the same set of customers. Avatar, which prides itself in personal consumer relations, is now trying to set up additional services to keep its current customers. It has recently upgraded its website, which formerly only allowed clients to update their personal information. Now clients can access information about their investments, income, and tax liabilities that is stored at the data center in Pennsylvania.

As a result of previous dealings, Avatar has been given free access to use the computer room of an older production plant. The company feels that this location is secure enough and would keep the data intact from physical intruders. The servers are housed in a room that the production plant used to house its legacy system. The room has detectors for smoke and associated sprinklers. It is enclosed with no windows and has specialized temperature-controlled air ducts.

Management has recently started looking at other alternatives to house the server as the plant is going to be shut down. Management has major concerns about the secrecy of the location and the associated measures. They want to incorporate newer methods of physical data protection. The company's auditors have also expressed a concern that some of the measures at the current location are inadequate and newer alternatives should be found.

Required:

1. Why are the auditors of Avatar stressing the need to have better physical environment for the server? If Avatar has proper software controls in place, would that not be enough to secure the information?
2. Name the six essential control features that contribute directly to the security of the computer server environment.

2. Internal Control

In reviewing the process procedures and internal controls of one of your audit clients, Steeplechase Enterprises, you notice the following practices in place. Steeplechase has recently installed a new computer system that affects the accounts receivable, billing, and shipping records. A specifically identified computer operator has been permanently assigned to each of the functions of accounts receivable, billing, and shipping. Each of these computer operators is assigned the responsibility of running the program for transaction processing, making program changes, and reconciling the computer log. To prevent any single operator from having exclusive access to the tapes and documentation, these three computer operators randomly rotate the custody and control tasks every two weeks over the magnetic tapes and the system documentation. Access controls to the computer room consist of magnetic cards and a digital code for each operator. Access to the computer room is not allowed to either the systems analyst or the computer operations supervisor.

The documentation for the system consists of the following: record layouts, program listings, logs, and error listings.

Once goods are shipped from one of Steeplechase's three warehouses, warehouse personnel forward shipping notices to the accounting department. The billing clerk receives the shipping notice and accounts for

the manual sequence of the shipping notices. Any missing notices are investigated. The billing clerk also manually enters the price of the item and prepares daily totals (supported by adding machine tapes) of the units shipped and the amount of sales. The shipping notices and adding machine tapes are sent to the computer department for data entry.

The computer output generated consists of a two-copy invoice and remittance advice and a daily sales register. The invoices and remittance advice are forwarded to the billing clerk, who mails one copy of the invoice and remittance advice to the customer and files the other copy in an open invoice file, which serves as an accounts receivable document. The daily sales register contains the total of units shipped and sales amounts. The computer operator compares the computer-generated totals to the adding machine tapes.

Required:
Identify the control weaknesses present and make a specific recommendation for correcting each of the control weaknesses.

3. Distributed Processing System

The internal audit department of a manufacturing company conducted a routine examination of the company's distributed computer facilities. The auditor's report was critical of the lack of coordination in the purchase of PC systems and software that individual departments use. Several different hardware platforms, operating systems, spreadsheet packages, database systems, and networking applications were in use.

In response to the internal audit report, and without consulting with department users regarding their current and future systems needs, Marten, the Vice President of Information Services issued a memorandum to all employees stating the following new policies:

1. The Micromanager Spreadsheet package was selected to be the standard for the company, and all employees must immediately switch to it within the month.
2. All future PC purchases must be Megasoft compatible.
3. All departments must convert to the Megasoft Entrée database package.
4. The office of the Vice President of Information Services must approve all new hardware and software purchases.

Several managers of other operating departments have complained about Marten's memorandum. Apparently, before issuing this memo, Marten had not consulted with any of the users regarding their current and future software needs.

Required:
a. When setting systems standards in a distributed processing environment, discuss the pertinent factors about:
   1. Computer hardware and software considerations.
   2. Controls considerations.
b. Discuss the benefits of having standardized hardware and software across distributed departments in the firm.
c. Discuss the concerns that the memorandum is likely to create for distributed users in the company.

4. Internal Control

Gustave, CPA, during its preliminary review of the financial statements of Comet, Inc., found a lack of proper segregation of duties between the programming and operating functions. Comet owns its own computing facilities. Gustave diligently intensified the internal control study and assessment tasks relating to the computer facilities. Gustave concluded in its final report that sufficient compensating general controls provided reasonable assurance that the internal control objectives were being met.

Required:
What compensating controls are most likely in place?

5. Disaster Recovery Plan

The headquarters of Hill Crest Corporation, a private company with $15.5 million in annual sales, is located in California. Hill Crest provides for its 150 clients an online legal software

service that includes data storage and administrative activities for law offices. The company has grown rapidly since its inception three years ago, and its data processing department has expanded to accommodate this growth. Because Hill Crest's president and sales personnel spend a great deal of time out of the office soliciting new clients, the planning of the IT facilities has been left to the data processing professionals.

Hill Crest recently moved its headquarters into a remodeled warehouse on the outskirts of the city. While remodeling the warehouse, the architects retained much of the original structure, including the wooden-shingled exterior and exposed wooden beams throughout the interior. The minicomputer distributive processing hardware is situated in a large open area with high ceilings and skylights. The openness makes the data processing area accessible to the rest of the staff and encourages a team approach to problem solving. Before occupying the new facility, city inspectors declared the building safe; that is, it had adequate fire extinguishers, sufficient exits, and so on.

In an effort to provide further protection for its large database of client information, Hill Crest instituted a tape backup procedure that automatically backs up the database every Sunday evening, avoiding interruption in the daily operations and procedures. All tapes are then labeled and carefully stored on shelves reserved for this purpose in the data processing department. The departmental operator's manual has instructions on how to use these tapes to restore the database, should the need arise. A list of home phone numbers of the individuals in the data processing department is available in case of an emergency. Hill Crest has recently increased its liability insurance for data loss from $50,000 to $100,000.

This past Saturday, the Hill Crest headquarters building was completely ruined by fire, and the company must now inform its clients that all of their information has been destroyed.

Required:

a. Describe the computer security weaknesses present at Hill Crest Corporation that made it possible for a disastrous data loss.
b. List the components that should have been included in the disaster recovery plan at Hill Crest Corporation to ensure computer recovery within 72 hours.
c. What factors, other than those included in the plan itself, should a company consider when formulating a disaster recovery plan?

6. Separation of Duties

Transferring people from job to job within the organization is the philosophy at Arcadia Plastics. Management feels that job rotation deters employees from feeling that they are stagnating in their jobs and promotes a better understanding of the company. The computer services personnel typically work for six months as an operator, one year as a systems developer, six months as a database administrator, and one year in systems maintenance. At that point, they are assigned to a permanent position.

Required:

Discuss the importance of separation of duties within the information systems department. How can Arcadia Plastics have both job rotation and well-separated duties?

7. Disaster Recover Service Providers

Visit SunGard's website, http://www.sungard.com, and research its recovery services offered for the following classes: High Availability, System Recovery, and End-User Recover. Write a report of your findings.

8. Audit Committee

Micro Systems, a developer of database software packages, is a publicly held company and listed with the SEC. The company has no internal audit function. In complying with SOX, Micro Systems has agreed to establish an internal audit function and strengthen its audit committee to include all outside directors. Micro Systems has held its initial planning meeting to discuss the roles of the various participants in the internal control and financial reporting process. Participants at the meeting included the company president, the chief financial officer, a member of the audit committee, a partner from Micro Systems' external audit firm, and the newly appointed manager of the internal audit

department. Comments from the various meeting participants are presented below.

President: We want to ensure that Micro Systems complies with SOX. The internal audit department should help to strengthen our internal control system by correcting problems. I would like your thoughts on the proper reporting relationship for the manager of the internal audit department.

CFO: I think the manager of the internal audit department should report to me because much of the department's work is related to financial issues. The audit committee should have oversight responsibilities.

Audit committee member: I believe we should think through our roles more carefully. The Treadway Commission has recommended that the audit committee play a more important role in the financial reporting process; the duties of today's audit committee have expanded beyond mere rubber-stamp approval. We need to have greater assurance that controls are in place and being followed.

External audit firm partner: We need a close working relationship among all of our roles. The internal audit department can play a significant role in monitoring the control systems on a continuing basis and should have strong ties to your external audit firm.

Internal audit department manager: The internal audit department should be more involved in operational auditing, but it also should play a significant monitoring role in the financial reporting area.

Required:

a. Describe the role of each of the following in the establishment, maintenance, and evaluation of Micro Systems' internal control.

   Management

   Audit committee

   External auditor

   Internal audit department

b. Describe the responsibilities that Micro Systems' audit committee has in the financial reporting process.

9. CMA 1290 4-Y8

Role of Internal Auditor

Leigh Industries has an internal audit department consisting of a director and four staff auditors. The director of internal audit, Diane Bauer, reports to the corporate controller, who receives copies of all internal audit reports. In addition, copies of all internal audit reports are sent to the audit committee of the board of directors and the individual responsible for the area of activity being audited.

In the past, the company's external auditors have relied on the work of the internal audit department to a substantial degree. However, in recent months, Bauer has become concerned that the objectivity of the nonaudit work that the department has performed is affecting the internal audit function. This possible loss of objectivity could result in external auditors performing more extensive testing and analysis. The percentage of nonaudit work that the internal auditors perform has steadily increased to about 25 percent of the total hours worked. A sample of five recent nonaudit activities is presented in the following section.

- One of the internal auditors assisted in the preparation of policy statements on internal control. These statements included such things as policies regarding sensitive payments and the safeguarding of assets.
- Reconciling the bank statements of the corporation each month is a regular assignment of one of the internal auditors. The corporate controller believes this strengthens the internal control function because the internal auditor is not involved in either the receipt or the disbursement of cash.
- The internal auditors are asked to review the annual budget each year for relevance and reasonableness before the budget is approved. At the end of each month, the corporate controller's staff analyzes the variances from budget and prepares explanations of these variances. The internal audit staff then reviews these variances and explanations.

- One of the internal auditors has been involved in the design, installation, and initial operation of a new computerized inventory system. The auditor was primarily concerned with the design and implementation of internal accounting controls and conducted the evaluation of these controls during the test runs.
- The internal auditors are sometimes asked to make the accounting entries for complex transactions as the employees in the accounting department are not adequately trained to handle such transactions. The corporate controller believes this gives an added measure of assurance to the accurate recording of these transactions.

Required:

a. Define objectivity as it relates to the internal audit function.

b. For each of the five nonaudit activities presented, explain whether the objectivity of Leigh Industries' Internal Audit Department has been materially impaired. Consider each situation independently.

c. The director of internal audit reports directly to the corporate controller.

1. Does this reporting relationship affect the objectivity of the internal audit department? Explain your answer.
2. Would your evaluation of the five situations in question b. change if the director of internal audit reported to the audit committee of the board of directors? Explain your answer.

10. Internal Control and Distributed System

Until a year ago, Dagwood Printing Company had always operated in a centralized computer environment. Now, 75 percent of the office employees have a PC. Users have been able to choose their own software packages, and no documentation of end-user-developed applications has been required. Next month, each PC will be linked into a local area network (LAN) and to the company's mainframe.

Required:

a. Outline a plan of action for Dagwood Printing Company to ensure that the proper controls over hardware, software, data, people, procedures, and documentation are in place.

b. Discuss any exposures the company may face if the above plan is not implemented.