CHAPTER 8

CONTROLLING INFORMATION SYSTEMS: INTRODUCTION TO PERVASIVE AND GENERAL CONTROLS

LEARNING OBJECTIVES

AFTER READING THIS CHAPTER, YOU SHOULD BE ABLE TO:

- DESCRIBE THE MAJOR PERVASIVE AND GENERAL CONTROLS THAT ORGANIZATIONS EMPLOY AS PART OF IT GOVERNANCE INITIATIVES.
- APPRECIATE HOW AN ORGANIZATION MUST PLAN AND ORGANIZE ALL RESOURCES, INCLUDING IT RESOURCES, TO ENSURE ACHIEVEMENT OF ITS STRATEGIC VISION.
- OVERVIEW THE MAJOR CONTROLS USED TO MANAGE THE DESIGN AND IMPLEMENTATION OF NEW PROCESSES, ESPECIALLY NEW IT PROCESSES.
- EXPLAIN CONTROLS THAT HELP ENSURE CONTINUOUS, RELIABLE BUSINESS AND IT PROCESSES.
- APPRECIATE THE INTEGRAL PART PLAYED BY THE MONITORING FUNCTION IN ENSURING THE OVERALL EFFECTIVENESS OF A SYSTEM OF INTERNAL CONTROLS.

On a trip from Perth, Australia to Kuala Lumpur, Malaysia a Malaysian Airlines jetliner suddenly, without being asked, zoomed up 3,000 feet. When the pilot took action to stop the climb, the plane was thrown, again without being asked, into a steep dive. When the pilot tried to counteract the dive, the plane sent itself into another steep climb. The pilot finally regained control and landed the plane safely. What happened? A defective software program, developed by Honeywell International Inc. for this Boeing 777, had provided incorrect data that confused the flight computer and caused it to send the plane and its 177 passengers on this roller coaster ride. Testing conducted by Honeywell during development of the software had failed to detect the responsible software bug.[1]

Amnon Jackont, an Israeli mystery novelist and history professor at Tel Aviv University, learned that friends and students were receiving e-mail messages from him that he had not sent. Also, unpublished portions of a book he was writing were discovered on Israeli

[1] Daniel Michaels and Andy Pasztor, "Incidents Prompt New Scrutiny of Airline Software Glitches," *The Wall Street Journal*, May 30, 2006, p. A1, A11.

Web sites. How was this happening? A *Trojan Horse* had been planted on Jackont's computer, and the computers and networks of 60 Israeli companies. The unauthorized changes to these computers had been perpetrated by members of three of the country's largest private investigation firms. The *computer fraud* charges against these perpetrators led to investigations of prestigious corporations for possibly stealing information from other companies. It seems that the purpose of the Trojan Horses was to steal data and sell it to competitors.[2]

An employee at Progressive Casualty Insurance Co. was interested in buying a new house and was looking for properties in foreclosure hoping to get a good deal. So, she wrongfully accessed information about foreclosure properties in Progressive's real estate database. Accessed data included names, social security numbers, birth dates, and property addresses. The employee was not authorized to view the data that she obtained, and this access was a failure of Progressive to comply with applicable privacy laws and regulations.[3]

When Hurricane Katrina struck New Orleans in August of 2005 some organizations were prepared for the ensuing disaster, and some were not. SCP Pool Corp.'s disaster recovery plan included the use of an emergency operations center in Dallas, 500 miles from SCP's headquarters in Covington, Louisiana. While operations did continue in Dallas after the hurricane, there were a few problems. A dozen application servers had to be retrieved from Covington and brought to Dallas after the storm. Fortunately, the Covington center survived the storm allowing this recovery. One problem that could not be solved was access to backup tapes stored at Iron Mountain, Inc.'s Kenner, Louisiana facility. The Iron Mountain facility was not accessible after the storm![4]

How are all of the stories related? These stories introduce the subject of this chapter, pervasive and general controls, because they are all failures of pervasive and general controls. As noted in Chapter 7, PCAOB Auditing Standard No. 2, paragraphs 50–53,[5] includes pervasive and general controls within "company-level controls" and emphasizes the pervasive affect that company-level controls have on the achievement of control objectives and the effectiveness of specific controls, such as business process controls. The standard goes on to give examples of four types of IT general controls. Each is represented in the preceding stories as follows:

- "Controls over computer program development" should include testing that is sufficient to detect errors in programs, such as the glitch in the Malaysian airliner's flight software.
- "Program change controls" include procedures to prevent *unauthorized* changes to computer programs such as the Trojan Horses at the Israeli companies.
- "Controls over access to programs and data" should include limiting access to data and other resources to only authorized personnel. The employee at Progressive was not authorized to obtain the data on foreclosed properties.
- "Controls over computer operations" should include contingency plans to allow organizations to continue to operate in the face of disasters such as hurricanes.

[2] Timothy L. O'Brien, "For a New Breed of Hackers, This Time Its Personnel," *The New York Times*, December 4, 2005, page 3.1.

[3] Jaikumar Vijayan, "Misuse of Insurer's Data Points to Inside Threats," *Computerworld*, April 17, 2006, p. 20.

[4] Lucas Mearian, "Hurricanes, Floods Put IT Staffs to the Test," *Computerworld*, September 5, 2005, pp. 1, 4–5.

[5] Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, PCAOB, March 9, 2004.

Synopsis

CONTROLS

This chapter describes several important pervasive controls and general controls (also known as IT general controls) that comprise a major element in *organizational governance* and *IT governance* initiatives. These controls protect an organization's resources, ensure that business processes operate as planned, and assist in the achievement of an organization's objectives.

ENTERPRISE SYSTEMS

E-BUSINESS

We begin by defining IT governance and describing management concerns about IT and the security threats posed by running organizations that are so highly dependent on IT for fulfilling their mission and achieving their objectives. Then, we introduce a hypothetical computer system and the information systems organization that operates that system. This system has multiple connections among the IT resources within and outside of the organization. Internal interconnectedness of this nature is typical of organizations employing *enterprise systems*. The external interfaces are typical of organizations engaged in *e-business*. The use of IT resources for enterprise systems and e-business magnifies the importance of protecting such resources from various risks. The interlinking of IT resources makes it much more difficult to provide protection, as compared to similar IT resources used in isolation.

We also will present four broad IT control process domains. These domains reflect groupings of control processes (i.e., management practices) that include, primarily, the pervasive and general controls that we want to discuss.

Introduction

In Chapter 7, we spent some time discussing *organizational governance* and *Enterprise Risk Management (ERM)* as an important organizational governance process. We also alluded to the relationship of IT governance and organizational governance. **IT governance** is the responsibility of executives and boards of directors, and consists of the leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.[6] We hope that you see the connections here. Organizational governance is about processes employed by organizations to select and attain objectives. IT governance is about processes to see that that the organization's IT supports the attainment of organizational objectives. Does good IT governance lead to better organizational performance? A study that examined IT governance processes and profitability at 256 companies found that businesses with superior IT governance practices generated 20 percent greater profits on average than other companies.[7]

How well does IT support organizational objectives? What are management's concerns about IT? A survey of 300 firms conducted by the Society for Information Management revealed these top 10 management concerns, all about IT's capability to support an organization's vision and strategy:[8]

1. IT and business alignment
2. Retaining IT professionals
3. Security and privacy
4. IT strategic planning

[6] *COBIT 4.0: Control Objectives for Information and Related Technology*, 4th ed. (Rolling Meadows, IL: IT Governance Institute, 2005): 6.

[7] Thomas Hoffman, "MIT Researchers Tie Good Governance to Higher Profits," *Computerworld*, July 12, 2004.

[8] "CIO Trendlines: Top Ten Management Concerns," *CIO Magazine*, February 1, 2005.

5. Speed and agility
6. Government regulation
7. Complexity reduction
8. IT governance
9. Information architecture (tied with number 8)
10. Business process reengineering

If we pursue concern number 3, security and privacy, we find a survey conducted of more than 8,200 respondents from 63 countries on 6 continents who reported the following top 10 strategic security concerns, all addressed by pervasive and general controls that provide assurance that resources are protected and objectives achieved:[9]

1. Disaster recovery/business continuity
2. Employee awareness programs
3. Data backup
4. Overall information security strategy
5. Network firewalls
6. Centralized security information management system
7. Periodic security audits
8. Monitoring employees
9. Monitoring security reports
10. Intellectual property protection

This chapter describes some of the typical pervasive and general controls—management practices/IT processes—employed to govern IT and to address the concerns and threats in the preceding list.

In Chapter 7, we defined *pervasive control plans* as those that relate to a multitude of control goals and processes. Like the control environment, also introduced in Chapter 7, pervasive control plans influence the effectiveness of the *business process control plans*. At the same time, *general controls/IT general controls* influence the effectiveness of *application controls.* For example, a general control plan that restricts access to data and programs stored on a computer can reduce the possibility that computer-based data (e.g., payroll or accounts receivable) will be altered without proper authorization. Thus, the general control, (restricting access to the computer) will have an impact on *any* application control intended to ensure the reliability of *any* related data. Recall that an organization establishes a system of controls to provide reasonable assurance that organizational objectives will be achieved (or, alternatively, that risks will be reduced or avoided). The system of controls consists of the control environment, pervasive control plans (and general controls), and business process control plans (and application controls). In this chapter, we describe some of the major pervasive and general controls employed by organizations.

In Chapter 7, we introduced COSO as a general framework for internal control. COSO is also the framework suggested by the PCAOB in Auditing Standard No. 2 as a suitable framework to guide management's assessment of internal control for SOX Section 404. No such recommendation was made for IT controls. However, one framework that has been widely adopted for IT governance and IT controls is COBIT (Control Objectives for Information and Related Technology). COBIT was developed by the IT Governance Institute to provide guidance—to managers, users, and auditors—on the best practices for the management of information technology. According to COBIT, IT resources must be managed by IT control processes to ensure that an

[9] Scott Berinato and Lorraine Cosgrove Ware, "The Global State of Information Security 2005," *CIO Magazine*, September 15, 2005.

EXHIBIT 8.1 IT Resources

Applications: Automated systems and manual procedures that process information.
Information: Data, in all their forms, that are input, processed, and output by information systems.
Infrastructure: Technology and facilities (hardware, operating systems, DBMSs, networking, multimedia, etc., and the environment that houses and supports them) that enable the processing of the applications.
People: Personnel who plan, organize, acquire, implement, deliver, support, monitor and evaluate information systems and services.

Source: Adapted from *COBIT 4.0: Control Objectives for Information and Related Technology*, 4th ed. (Rolling Meadows, IL: IT Governance Institute, 2005): 13.

organization has the information it needs to achieve its objectives. Exhibit 8.1 defines the IT resources that must be managed, and Chapter 1 (especially Figure 1.6, pg. 19, and Exhibit 1.2, pg. 20) describes the qualities that this information must exhibit for it to be of value to the organization. COBIT thus supports IT governance by providing a framework to ensure that:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately.[10]

Because the COBIT framework is a major source for the control processes described in this chapter, we should include here the COBIT definition for control:[11]

> The policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

Let's compare this definition to those proposed by COSO and this textbook. Notice that all three definitions refer to the achievement of objectives. COSO and the textbook definitions make these objectives explicit, whereas the COBIT objectives are the qualities of information introduced in Chapter 1. Finally, the COBIT definition adds the idea that controls should address "undesired events." This is similar to our assertion here and in Chapter 7 that internal controls, and in this particular instance IT processes, should reduce the possibility that risks will occur.

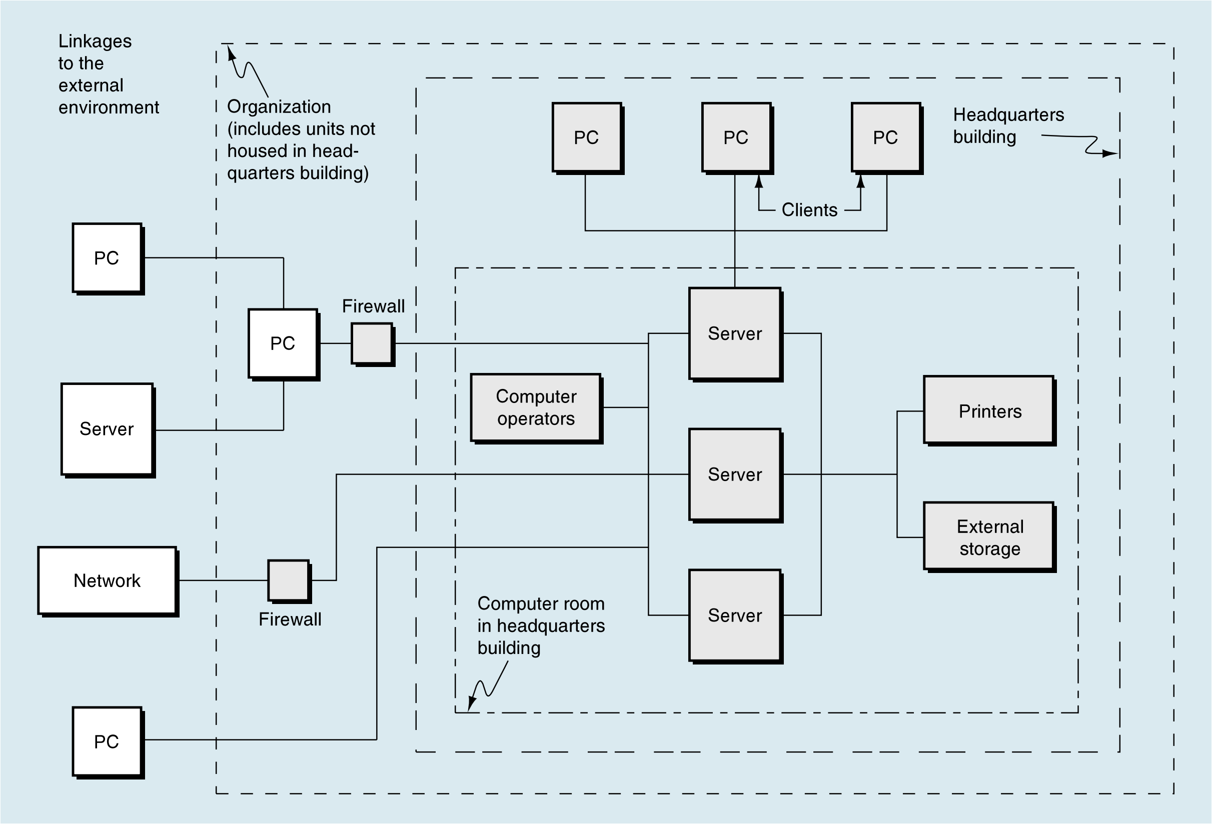
A Hypothetical Computer System

The IT resources are typically configured with some or all of the elements shown in Figure 8.1 (pg. 248), which we will use to focus our discussions. This computer system consists of one or more *servers* clustered together and housed in a computer room within the organization's headquarters. This computer is connected to printers, external storage devices, and PCs, sometimes referred to as *clients*, located within the building, and to PCs located in the organization's other facilities. All of these connections are via networks, often referred to as *local area networks (LANs)* or *wide area networks (WANs)*.

[10] *COBIT 4.0: Control Objectives for Information and Related Technology*, 4th ed. (Rolling Meadows, IL: IT Governance Institute, 2005): 7.

[11] *COBIT 4.0: Control Objectives for Information and Related Technology*, 4th ed. (Rolling Meadows, IL: IT Governance Institute, 2005): 17.

FIGURE 8.1 A Hypothetical Computer System


Linkages to the external environment
Organization (includes units not housed in head-quarters building)
PC
PC
PC
Headquarters building
Clients
PC
Server
PC
Firewall
Server
Computer operators
Printers
Server
External storage
Network
Firewall
Computer room in headquarters building
Server
PC

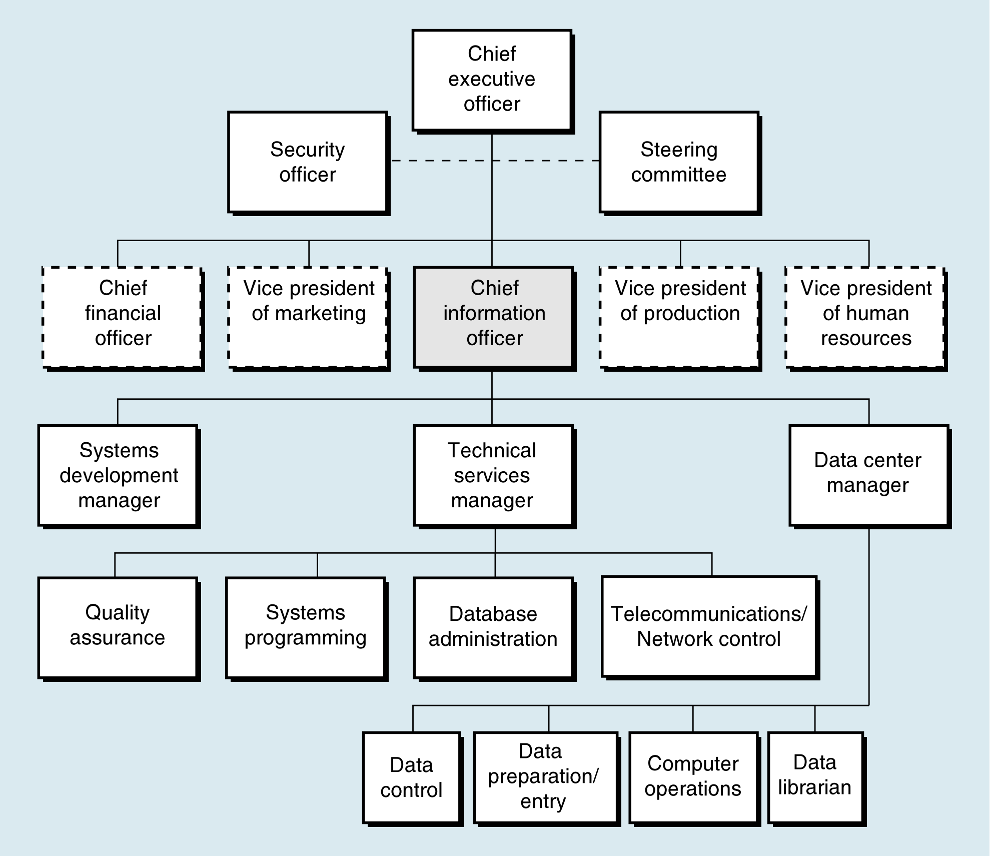
Finally, computer facilities operated by other organizations are connected, perhaps via the *Internet* and through *firewalls*, to the internal servers, PCs, and other equipment.

Controlling the operation of this configuration provides many challenges to the organization. To support organizational objectives and to provide an environment in which business process control plans can be effective, we must determine how we can protect the computer from misuse, whether intentional or inadvertent, from inside and outside the organization. Furthermore, how do we protect the computer room, the headquarters building, and the rooms and buildings in which other connected facilities are located? In the event of a disaster, do we have plans in place for continuing our operations? What policies and procedures should be established (and documented) to provide for efficient, effective, and authorized use of the computer? What measures can we take to help ensure that the personnel who operate and use the computer are competent and honest? Answers to these and similar questions run to the heart of IT control processes. This chapter addresses these issues.

The Information Systems Organization

Before we begin the discussion of IT control processes, however, we need to take a look at the information systems organization, which is the department or function that develops and operates an organization's information system. The function (department) is composed of people, procedures, and equipment, and it is typically called the *information systems department*, *IS department*, or *IT department*. Figure 8.2 depicts a typical IT department. This type of structure places the information systems function under the

FIGURE 8.2 Information Systems Organization



line authority of the chief information officer or CIO (also known as the vice president of information systems).

Table 8.1 (pg. 250) outlines the principal responsibilities, major duties, and key control concerns related to each functional box depicted in Figure 8.2. We include key control concerns in Table 8.1 to raise your awareness of control issues related to particular functional activities and to the organization of the information system as a whole.

Take some time now to study Figure 8.2 and Table 8.1. Be sure you have a good understanding of the principal responsibilities, major duties, and key control concerns of each functional title.

The remainder of the chapter presents the four broad domains of IT control processes. As we discuss these pervasive and general controls, we will present them as plans designed to increase the likelihood that objectives will be achieved and that risks will be avoided. The discussion will be sprinkled with actual case examples of system breakdowns caused by both unintentional acts and intentional (malicious) acts. Also, we will occasionally allude to the control goals and information qualities that the IT control processes help an organization achieve.

Four Broad IT Control Process Domains

COBIT groups IT control processes into four broad domains: (1) Plan and Organize, (2) Acquire and Implement, (3) Deliver and Support, and (4) Monitor and Evaluate. Figure 8.3 (pg. 251) depicts the relationship of these four domains and lists the IT

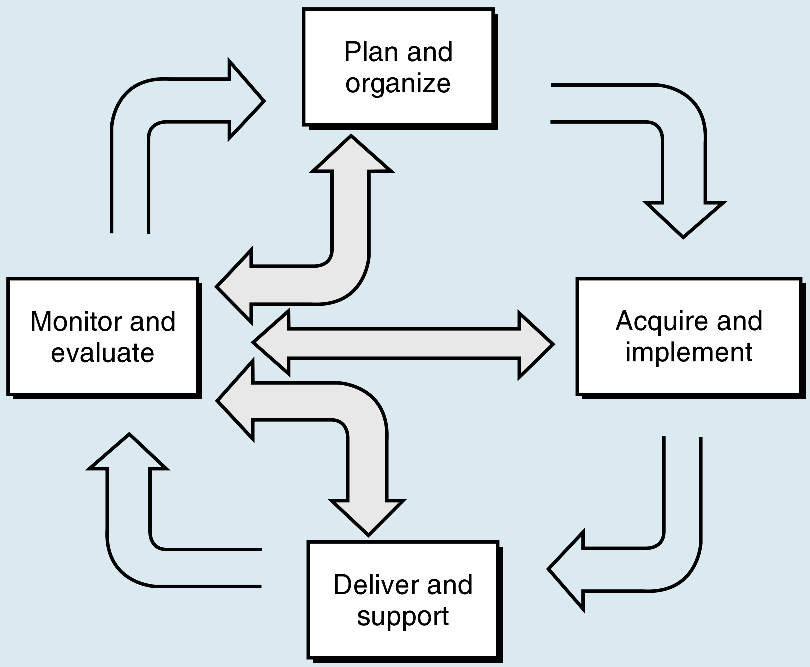
TABLE 8.1 Summary of IT Organization Functions

Functional Title (see Figure 8.2)	Principal Responsibilities	Major Duties	Key Control Concerns
Steering committee	Guide and advise IT.	Prioritize and select IT projects and resources.	Organization and IT strategic objectives are misaligned.
Security officer	Ensure the security of all IT resources.	Physical security (e.g., building and computer) and logical security (enterprise data).	Disasters (e.g., hurricanes, terrorist attacks, power outages, fires, hackers).
Chief information officer	Efficient, effective operation of IT. Alignment of IT resources and organization objectives.	Plans IT acquisition and development; controls IT operations.	IT function fails to support organization's mission.
Systems development manager	Delivers cost-effective, bug-free applications.	Supervises applications systems development; sets and monitors multiple project deadlines.	Systems development can develop and implement systems without management or user approval.
Technical services manager	Manages miscellaneous specialized and technical functions.	Manages functional units such as networks, computer-aided design/computer-aided manufacturing (CAD/CAM), and systems programming.	Access to this technology is a vulnerable point in the information system.
Quality assurance	Maintains quality management standards and systems. Ensures continuous improvement of systems development and data quality.	Conducts reviews to determine adherence to IT standards and procedures and achievement of IT objectives.	Developed systems fail to achieve objectives. Projects not completed on time and within budgets. Data fails to satisfy quality criteria.
Systems programming	Maintains systems software.	Modifies and adapts systems software, including operating systems and various utility routines.	Systems programmers can easily access applications programs and data.
Database administration (DBA)	Designs and controls the database.	Maintains database software; monitors and controls access to the database.	DBA is the central point from which to control data *and* is a central point of vulnerability.
Telecommunications/ Network control	Installs and supports organizational telecommunications and network hardware and software.	Acquires, installs, maintains, and secures telecommunications and network hardware and software.	Less than optimal performance of telecommunications and networks. Security breaches.
Data center manager	Plans, controls, and delivers IT production activities.	Monitors computer operations; hires, schedules, and oversees personnel on multishift operations.	Systems development activities undertaken by operations personnel can bypass normal controls.
Data control	Routes all work into and out of the data center; corrects errors; monitors all error correction.	Checks input and output batches for validity, completeness, and accuracy; distributes output.	An independent data control function ensures valid, complete, and accurate processing.
Data preparation/entry	Prepares input for computer processing.	Keys data directly into computer; uses offline devices to record data on magnetic or optical disks.	High risk of data conversion errors, which have pervasive impact.

TABLE 8.1 (*Continued*)

Functional Title (see Figure 8.2)	Principal Responsibilities	Major Duties	Key Control Concerns
Computer operations	Provides efficient and effective operation of the computer equipment.	Mounts tapes, disks, and other media; monitors equipment operation.	An operator allowed to program the computer can make unauthorized software changes.
Data librarian	Maintains custody of and controls access to programs, files, and documentation.	Issues programs, data, and documentation to authorized users; maintains record of data, program, and documentation usage.	Controlled access to data, programs, and documentation reduces unauthorized program changes and unauthorized computer operations.

FIGURE 8.3 Four Broad IT Control Process Domains (from COBIT) and Ten Important IT Control Processes



IT Control Processes and Domains

Domain	Plan and Organize	Acquire and Implement	Deliver and Support	Monitor and Evaluate
IT Control Process	1. Establish strategic vision for IT. 2. Develop tactics to plan, communicate, and manage relization of the strategic vision.	3. Identify automated solutions. 4. Develop and acquire IT solutions. 5. Integrate IT solutions into operational processes. 6. Manage changes to existing IT systems.	7. Deliver required IT servies. 8. Ensure security and continuous service. 9. Provide support sevices.	10. Monitor and evaluate the processes.

control processes within each domain, for a total of 10 processes. Notice that the Monitor and Evaluate domain provides feedback to the other three domains.

Before we move on to a discussion of the 10 IT control processes, let's discuss the concept of a control process. First, a "control process" could easily be, and often is, referred to as a "management practice." This latter terminology emphasizes management's responsibility for control in the organization and the practices or processes that will bring about achievement of an organization's objectives. Second, the prominence of "process" in this terminology reminds us of the definition of control as "a process." It is through a coordinated effort, across all IT resources and all organizational units, that the objectives of the organization are achieved.

Plan and Organize Domain

Within the Plan and Organize domain are processes to develop the strategy and tactics for realizing an organization's IT strategy. The overriding goal of these processes is to identify ways that IT can best contribute to the achievement of the organization's objectives. After a strategic vision is set, management must communicate the vision to affected parties (inside and outside the organization) and put in place the IT organization and technology infrastructure that enables that vision. These processes must identify and address external threats and internal and external IT requirements, and identify and take advantage of opportunities for strategic implementation of emerging information technology.

IT Process 1: Establish Strategic Vision for Information Technology

To strike an optimal balance of IT opportunities and IT business requirements, management of the information services function should adopt a process for developing a strategic plan for all of the organization's IT resources and for converting that plan into short-term goals. The information systems strategic planning effort must ensure that the organization's strategic plan is supported and that information technology is used to the best advantage of the organization. An organization wants to be sure that the information systems function is prepared to anticipate the competition's actions and to take advantage of emerging information technology. An organization must establish links between organizational and information systems strategic planning to ensure that strategies plotted in the organizational plan receive the IT support they need.

Strategic planning processes, and corresponding elements of strategic IT plans, include the following:

1. *A summary of the organizational strategic plan's goals and strategies, and how they are related to IT:* This information is included to provide a framework for the strategic IT plan and to make sure that the plan is directed toward achieving organizational objectives (see next item).
2. *IT goals and strategies, and a statement of how each will support organizational goals and strategies:* These strategies include a description of major information subsystems and applications. Mission-critical applications—those IT applications central to the successful competitive performance of the organization—must be separately identified and monitored.

E-BUSINESS

ENTERPRISE SYSTEMS

3. *An information architecture model encompassing the corporate data model and the associated information systems:* Plans for any new lines of business, such as e-business, or changes in business processes, such as change over to an enterprise system, will require new

data and relationships among the data. These data elements and relationships must be incorporated into the organization's information architecture model.

4. *An inventory of current IT capabilities:* The inventory should include hardware (computers and networks), software, personnel (quantities and skills), application systems, utilization rates, strengths, and weaknesses. This inventory should address both primary and backup facilities. A process must be in place to review IT capabilities to ensure that there is adequate technology to take advantage of emerging technology.
5. *Acquisition and development schedules for hardware, software, and application systems and for personnel and financial requirements:* These should be stated in detail for the following one or two years and should provide a basis for specific actions and for control.
6. *IT-related requirements to comply with industry, regulatory, legal, and contractual obligations, including safety, privacy, transborder data flows, e-business, and insurance contracts:* To avoid fines, sanctions, and loss of business, the organization must maintain procedures to ensure awareness and compliance with these obligations.
7. *IT risks and the risk action plan:* To ensure the achievement of IT objectives, in support of business objectives, and to respond to threats to the provision of IT services, management should establish a risk-assessment framework, including risk identification, measurement, actions, and the formal acceptance and communication of the residual risk.
8. *Process for modifying the plan to accommodate changes to the organization's strategic plan and changes in IT conditions:* The strategic IT plan should not be a static document. Rather, it should be kept up to date to accommodate changes in organizational objectives and to leverage opportunities to apply information technology for the strategic advantage of the organization.

E-Business

IT Process 2: Develop Tactics to Plan, Communicate, and Manage Realization of the Strategic Vision

To ensure adequate funding for IT, controlled disbursement of financial resources, and effective and efficient utilization of IT resources, an organization must manage IT resources by using IT capital and operating budgets, by justifying IT expenditures, and by monitoring costs (in light of risks).

To ensure the overall effectiveness of the IT function, management must establish a direction and related policies addressing such aspects as positive control environment throughout the organization, code of conduct/ethics, quality, and security. Then, these policies must be communicated (internally and externally) to obtain commitment and compliance. IT management's direction and policies must be consistent with the *control environment* established by the organization's senior management.

To ensure that projects are undertaken in order of importance, completed on time, and completed within budget, management must establish a project-management framework to ensure that project selection is in line with plans and that a project-management methodology is applied to each project undertaken.

Management should establish a quality assurance (QA) plan and implement related activities, including reviews, audits, and inspections, to ensure the attainment of IT customer requirements. A systems development life cycle methodology (SDLC) is an essential component of the QA plan.

To ensure that IT services are delivered in an efficient and effective manner, there must be adequate internal and external IT staff, administrative policies and procedures for all functions (with specific attention to organizational placement, roles and responsibilities, and segregation of duties), and an IT steering committee to determine prioritization of resource use. We divide these controls into two groups: *organizational control plans* and *personnel control plans*.

Organizational Control Plans

We will concentrate on two organizational control plans: segregation of duties and the information systems function.

Segregation of Duties Control Plan. Without proper segregation of duties, an organization might fail to achieve the control goals of *input accuracy* or *update accuracy*, leading to erroneous financial and other data. For example, assume that one person is responsible for recording all the data necessary to recognize a sales event. If that person were to make a mistake, then the stored data and output reports, such as the financial statements, would be misstated because no one else would have checked this person's work. This control plan also helps to ensure *security of resources*. For example, the CEO and CFO of WorldCom, Inc. thwarted the system of internal controls by authorizing, executing, and recording false accounting transactions that resulted in bogus inflated revenues totaling around $11 billion. The board of directors, which is supposed to serve as a "watchdog" over upper management, was so passive that it failed to uncover the fraud that was taking place under its very nose.[12] The entire system of internal control and corporate governance apparently imploded at WorldCom.

Segregation of duties consists of separating the four basic functions of event processing:

- *Function 1:* Authorizing events.
- *Function 2:* Executing events.
- *Function 3:* Recording events.
- *Function 4:* Safeguarding resources resulting from consummating events.

The concept underlying segregation of duties is simple enough. Through the design of an appropriate organizational structure, no single employee should be in a position both to perpetrate and conceal frauds, errors, or other kinds of system failures. A brief scenario should illustrate this point. John Singletary works in the general office of Small Company. He initiates a sales order and sends the picking ticket to the warehouse, resulting in inventory being shipped to his brother. When Sue Billings sends Singletary the customer invoice for the shipment, he records the sale as he would any sale. Sometime later, he writes his brother's account off as a bad debt. What is the result? Inventory was stolen, and Singletary manipulated the information system to hide the theft. Had other employees been responsible for authorizing and recording the shipment or for the bad debt write-off, Singletary would have had a tougher time manipulating the system.

Table 8.2 illustrates segregation of duties in a manual system. Examine the top half of the table, which defines the four basic functions. The bottom half of the table extends the coverage of segregation of duties by illustrating the processing of a credit sales event.

Let's examine Table 8.2 as a means of better understanding the control notion underlying segregation of duties. Ideal segregation of duties requires that different units (departments) of an organization carry out each of the four phases of event processing. In this way, *collusion* would need to occur between one or more persons (or departments) to exploit the system and conceal the abuse. Whenever collusion is necessary to commit a fraud, a greater likelihood exists that the perpetrators will be deterred by the risks associated with pursuing a colluding partner. Thus, at a minimum, an organization must

[12] Jim Hopkins, "Report: WorldCom Board Passive," *USA Today—Business* (June 10, 2003).

TABLE 8.2 Illustration of Segregation of Duties

Function 1	Function 2	Function 3	Function 4
Authorizing Events	**Executing Events**	**Recording Events**	**Safeguarding Resources Resulting from Consummating Events**
Activities • Approve phases of event processing.	• Physically move resources. • Complete source documents.	• Record events in books of original entry. • Post event summaries to the general ledger.	• Physically protect resources. • Maintain accountability of physical resources.
Example: Processing a credit sales event			
Activities • Approve customer credit. • Approve picking inventory and sending inventory to shipping department. • Approve shipping inventory to customer. • Approve recording accounting entries.	**Physical Movement Resources** • Pick inventory from bins. • Move inventory from warehouse to shipping department. • Ship inventory to customer. **Complete Source Documents** • Complete sales order. • Complete shipping document. • Complete invoice.	**Record Event Details** DR AR–A/R Subsidiary Ledger CR Sales–Sales Journal DR Cost of Goods Sold–Inventory Ledger CR Inventory–Inventory Ledger **Post Event GL Summaries** DR AR CR Sales DR Cost of Goods Sold CR Inventory	**Physically Protect** • Safeguard inventory while in storage at warehouse, while in transit to shipping department, and while being prepared for shipment to customer. **Maintain Accountability** • Examine and count inventory periodically, and compare physical total to recorded total.

be large enough to support at least four independent units to implement segregation of duties *effectively*.

In practice, the customer service department might be responsible for accepting customer orders and completing sales orders. The credit department might be responsible for determining the existence of customers and approving their creditworthiness. The warehouse might be responsible for safeguarding inventory while it is being stored. The shipping department might be responsible for protecting inventory while it is awaiting shipment and for executing the shipment.

But how do we accomplish this in small organizations that have few employees? Perhaps we don't. At a minimum, we should strive to separate the critical duties. Also, in this kind of environment, we would place greater reliance on personnel control plans aimed at hiring honest employees and motivating those people to stay honest, coupled with close supervision by top management. These alternative control plans are commonly called *compensatory controls*.

E-BUSINESS

Controls to prevent *unauthorized* execution of events help prevent *fraud* by ensuring that only *valid* events are recorded. Therefore, function 1, authorizing events, takes on particular significance in our segregation of duties model. Control plans for authorizing or approving events empower individuals or computers to initiate events and to approve actions taken subsequently in executing and recording events. Authorization control plans often take the form of policy statements and are implemented by including necessary procedures and business process controls within the information system that will process the events. For example, through proper design of the sales order form, an organization can see that credit is granted by including a block on the document that requires the credit manager's signature. Or, a computer-based system can be designed to approve sales within some predetermined credit limits. In some e-business trading partner arrangements, a retail store's computer is authorized to automatically send a stock replenishment order to a vendor when shelf inventory runs low. The vendor's computer automatically sends the goods to the retail store. In turn, the retail stores' computer automatically receives the goods and pays the vendor. In this example, computer-based rules authorized the purchase, sale, movement, and receipt of goods. These procedures receive management authorization when the system is approved during initial development or when the system is changed.

Although consolidating authorization, execution, and recordkeeping functions within IT may appear to be a bad idea, it may serve to *increase* internal control. For example, automated credit checks to *authorize* sales will—if the programs are tested and implemented properly—be *consistently* performed on *every* sale. The sales order will not be prepared (i.e., *execute)* and sent to shipping unless the credit check has been performed. Finally, the sale will not be *recorded* unless an authorized person (e.g., a shipping clerk) enters the shipment. The system can also keep a record of when and by whom each step was performed. Thus, during a SOX 404 review of internal controls, this automated segregation of duties can be tested to determine that the controls are in place (i.e., they are in the programs) and have been performed (the audit trail). This automation of segregation of duties may be a more *efficient* and *effective* system of internal control. In the next section, we describe the segregation that must exist *within IT* for such controls to be effective.

Organizational Control Plans for the IT Organization. The IT organization normally acts in a service capacity for other operating units in the organization. In this role, it should be limited to carrying out function 3 of Table 8.2 (pg. 255) recording events and posting event summaries. Approving and executing events along with safeguarding resources should be carried out by departments other than IT. This arrangement allows for the effective implementation of *segregation of duties*. Situations exist, however, where the functional divisions we mentioned previously can be violated. For instance, some IT systems do authorize and execute events; for example, the computer might be programmed to approve credit sales, purchases, receipts, and payments, as previously mentioned. However, with this example, the authorization actually occurred when an authorized manger developed and implemented the computer-based rules. And, the safeguarding of assets (inventory received) was in the hands of the receiving function. Any changes to such rules must be restricted to authorized persons only who are not part of IT.

Within IT, we segregate duties to control unauthorized use of and/or changes to the computer and its stored data and programs. Segregation of duties within IT can be accomplished in a number of ways. For example, in examining Figure 8.2 (pg. 249), we see that *systems development*, *technical services*, and the *data center manager* are segregated. A method of separating systems development and operations is to prevent programmers from operating the computer, thus reducing the possibilities of unauthorized data input or unauthorized modification of stored data and programs.

The data librarian also assists in separating key functions. For example, a librarian function grants access to stored data and programs to authorized personnel only. This separation reduces the risk of unauthorized computer operation or unauthorized programming by operators. Librarian controls, combined with restricting access to the database and making the *security officer* responsible for assigning *passwords*, are critical to separating key functions within IT and limiting access to computing resources.

In addition to assigning passwords, the **security officer** might perform a multitude of control-related activities such as monitoring employees' network access, granting security

Technology Application 8.1

IT STEERING COMMITTEES

Case 1

MasterCard International Inc.'s IT steering committee includes IT representatives and business managers from each operating region. The committee meets every six weeks to categorize and rank proposed IT projects based on business needs and projected paybacks.

Case 2

Novell, Inc. and FedEx Corp. have elevated IT governance to the board of directors. The IT steering committees at these organizations include board members and oversee major IT-related projects and architecture decisions.

Case 3

Allstate Insurance Co. has created an IT governance committee that includes the chairman and CEO (Chief Executive Officer) and CFO (Chief Financial officer). This committee decides how to prioritize IT initiatives based on business needs.

Source: Thomas Hoffman, ''IT Execs Downplay Role of Sarbanes-Oxley in Governance,'' *Computerworld,* July 12, 2004; Thomas Hoffman, ''IT Oversight Gets Attention at Board Level,'' *Computerworld,* May 17, 2004; Thomas Hoffman, ''IT Governance Is on the Hot Seat,'' *Computerworld,* July 12, 2004.

clearance for sensitive projects, and working with human resources to ensure that interview practices, such as thorough background checks, are conducted during the hiring process.

The senior management in many organizations appoints a committee to oversee IT and its activities. This **IT steering committee** coordinates the organizational and IT strategic planning processes and reviews and approves the strategic IT plan. The steering committee can provide significant help to the organization in establishing and meeting user information requirements and in ensuring the effective and efficient use of the organization's IT resources. The committee should consist of about seven executives from major functional areas of the organization, including the CIO; report to senior management; and meet regularly. Technology Application 8.1 describes some effective IT steering committees.

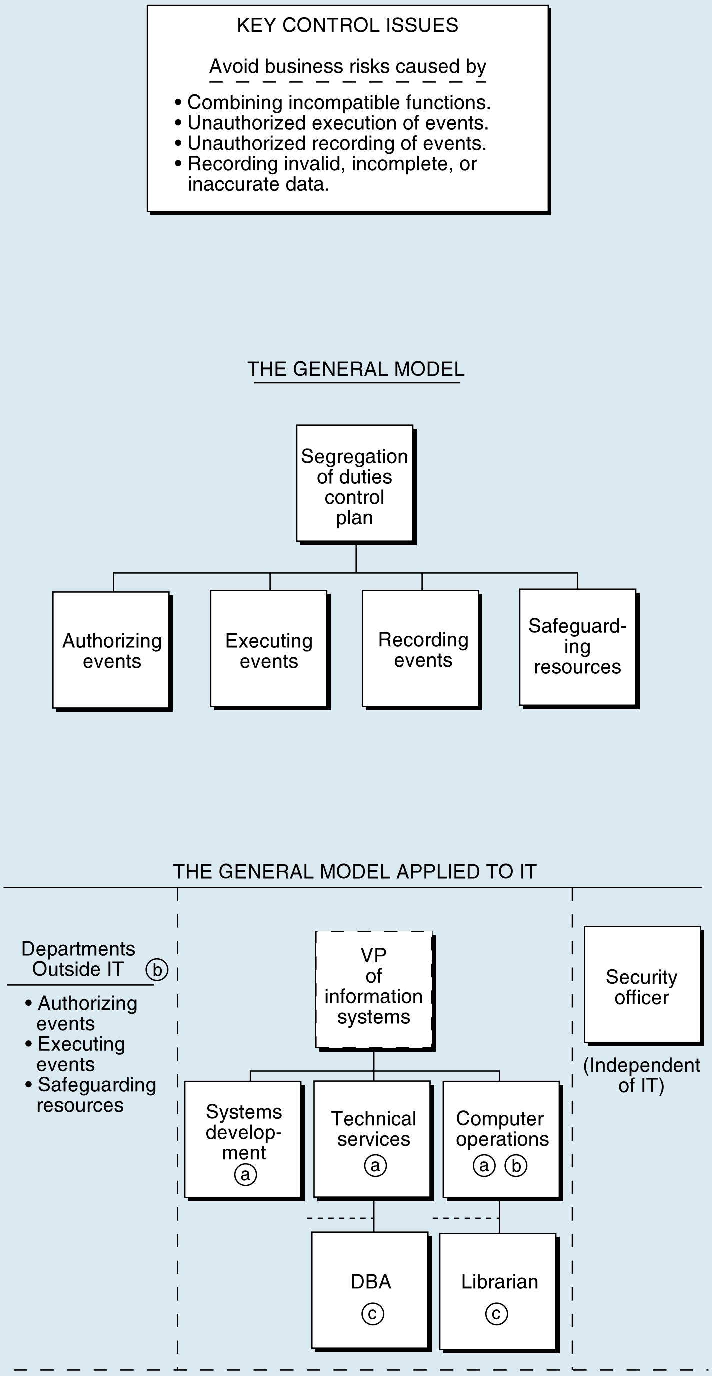
Figure 8.4 (pg. 258) provides a summary of the preceding discussion. Because this section deals with organizational control plans, the figure is presented in the form of two organization charts—one general and one specific to IT—preceded by a summary of the key control issues presented in this section.

Personnel Control Plans

All personnel, including IT personnel, must be managed to maximize their contributions to the organization and IT. Specific attention must be paid to recruitment, promotion, personnel qualifications, training, backup, performance evaluation, job change, and termination. As we discussed earlier in the chapter, an organization that does not have a critical mass of honest, competent employees will find it virtually impossible to implement other control plans.

Personnel control plans help to protect an organization against certain types of risks. For example, hiring incompetent employees could result in time and money being wasted on futile training programs. Alternatively, offering employment to an individual unqualified to fill a position may preclude efficient, effective operations or, if the person cannot follow instructions, may lead to inaccurate information processing. Obviously, hiring an employee with a prior record of dishonesty exposes the organization to a greater possibility of *fraud*.

FIGURE 8.4 Summary of Organizational Control Plans



NOTES:

ⓐ Divorce these three functions from one another.

ⓑ Computer operations limited to the function of *recording events.*

ⓒ DBA (Database administration) and librarian functions play key roles in restricting access to computer resources.

FIGURE 8.5 Summary of Personnel Control Plans

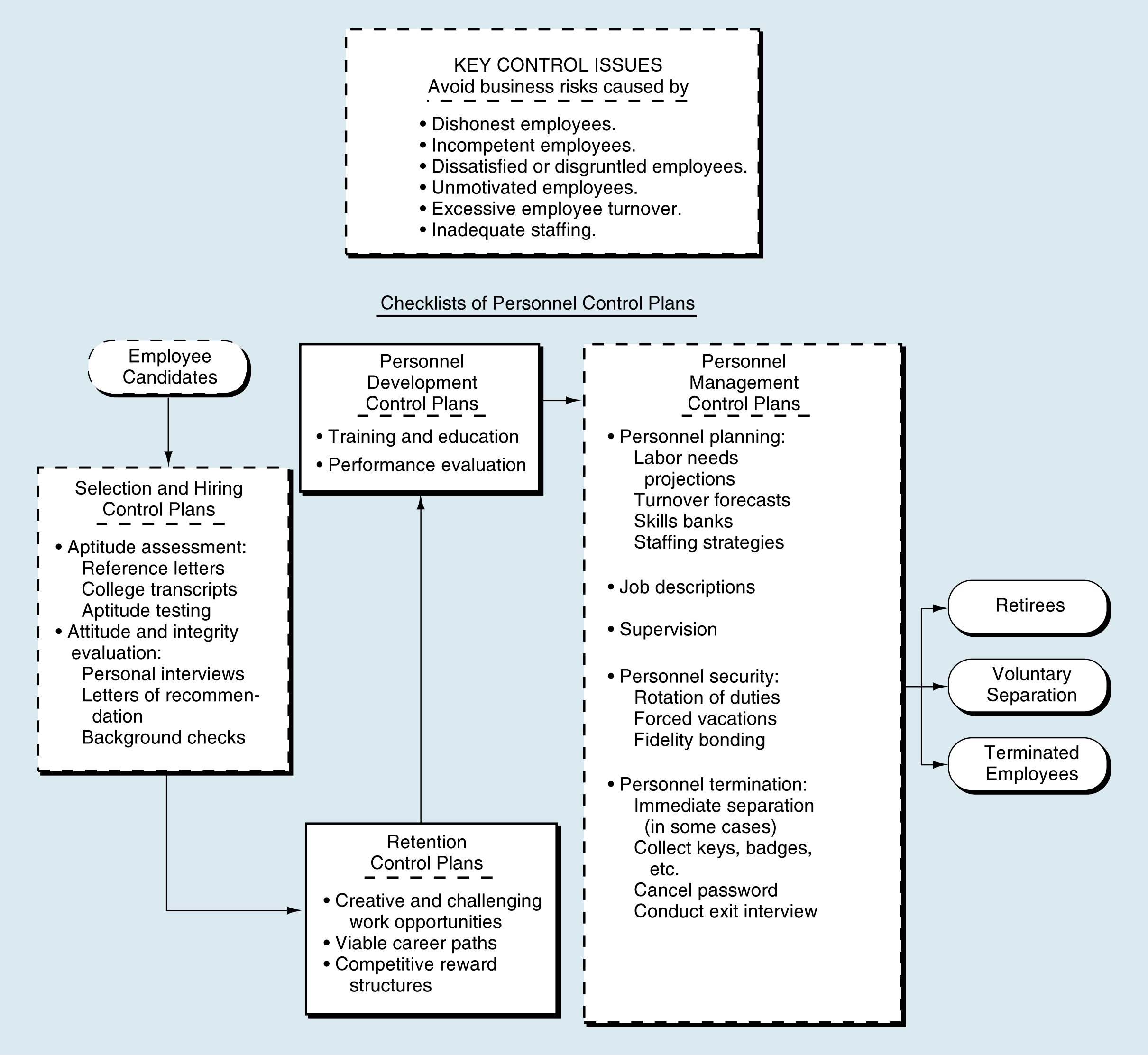

KEY CONTROL ISSUES
Avoid business risks caused by
• Dishonest employees.
• Incompetent employees.
• Dissatisfied or disgruntled employees.
• Unmotivated employees.
• Excessive employee turnover.
• Inadequate staffing.
Checklists of Personnel Control Plans
Employee Candidates
Selection and Hiring Control Plans
• Aptitude assessment: Reference letters College transcripts Aptitude testing
• Attitude and integrity evaluation: Personal interviews Letters of recommendation Background checks
Personnel Development Control Plans
• Training and education
• Performance evaluation
Retention Control Plans
• Creative and challenging work opportunities
• Viable career paths
• Competitive reward structures
Personnel Management Control Plans
• Personnel planning: Labor needs projections Turnover forecasts Skills banks Staffing strategies
• Job descriptions
• Supervision
• Personnel security: Rotation of duties Forced vacations Fidelity bonding
• Personnel termination: Immediate separation (in some cases) Collect keys, badges, etc. Cancel password Conduct exit interview
Retirees
Voluntary Separation
Terminated Employees

Figure 8.5 summarizes a number of personnel control plans aimed at mitigating the effects of these types of risks. As you study each plan, think of the risks that the plan can prevent or the control goal that could be achieved by implementing the plan.

Selection and Hiring Control Plans. Candidates applying for positions should be carefully screened, selected, and hired. The requirement for a technical background and the shortage of qualified applicants make the selection and hiring of systems personnel particularly important.

Retention Control Plans. Retaining qualified personnel can be even more difficult than hiring them. Again, the problem is especially critical when dealing with systems personnel. Companies should make every effort to provide creative and challenging work opportunities and, when possible, to offer open channels to management-level positions.

Personnel Development Control Plans. Training must be regular, not haphazard. Deficiencies noted in an employee's background should be rectified through proper training or education. Training must be preeminent in an employee's work schedule. In general, performance reviews are performed for at least four reasons. First, a review determines whether an employee is satisfying the requirements of a position as indicated by a job description. Second, it assesses an employee's strengths and weaknesses. Third, it assists management in determining whether to make salary adjustments and whether to promote an employee. Finally, it identifies opportunities for training and for personal growth.

Personnel Management Control Plans. *Personnel planning control plans* project future managerial and technical skills of the staff, anticipate turnover, and develop a strategy for filling necessary positions. *Job description control plans* lay out the responsibilities for each position on an organization chart and identify the resources to be used in performing those responsibilities. *Supervision control plans* involve the processes of approving, monitoring, and observing the work of others.

Personnel security control plans prevent the organization's own personnel from committing acts of computer abuse, fraud, or theft of assets. **Rotation of duties** is a policy that requires an employee to alternate jobs periodically. **Forced vacations** is a policy that requires an employee to take leave from the job and substitutes another employee in his or her place. The control notion underlying these plans is that if an employee is perpetrating some kind of irregularity, that irregularity will be *detected* by the substitute. Furthermore, if these plans are in place, they should act as a deterrent to the irregularity ever occurring in the first place (i.e., preventive). Beyond the control considerations involved, these two plans also help mitigate the disruption that might be caused when an employee leaves the organization. Because another person(s) is familiar with the job duties of each position, no single employee is irreplaceable.

What if personnel security control plans fail to prevent employee dishonesty? By bonding their key employees, many organizations insure against the financial losses that could result. A **fidelity bond** indemnifies a company in case it suffers losses from defalcations committed by its employees. Employees who have access to cash and other negotiable assets are usually bonded.

Termination control plans define the set of procedures a company follows when an employee voluntarily or involuntarily leaves an organization. Although all departments within a company should implement termination policies, rigorous application of these policies is particularly important in IT. Disgruntled employees working in the IT have the opportunity to cause much damage in a short time. For example, computer operations personnel could erase large amounts of stored data in a matter of minutes. For this reason, key employees who have access to important stored data and programs may be asked to leave the facility immediately, and in some cases, company security personnel may escort them off the premises.

Acquire and Implement Domain

Processes within the Acquire and Implement domain are designed to identify, develop or acquire, and implement IT solutions, and integrate them into the business process. Once installed, procedures must also be in place to maintain and manage changes to existing systems. Failure to successfully execute these processes can lead to significant risks throughout the organization. For example, if we do not correctly determine the requirements for a new information system *and* see that those requirements are satisfied by the new system, the new system could cause us to violate accounting standards or perform calculations incorrectly that lead to incorrect financial reporting. Or we may not complete the development on time, putting us at a competitive disadvantage if our competition implements such a system first and within budget. Finally, should we fail to develop proper controls for the new system, we could experience several risks, including erroneous financial reporting, fraud, and loss of resources.

Our discussion of this domain is brief here because these processes are analyzed in depth in Chapter 17. The following discussion often refers to the **systems development life cycle (SDLC)**, which is the progression of information systems *through* the systems development process, from birth, through implementation, to ongoing use.

IT Process 3: Identify Automated Solutions

To ensure the selection of the best approach to satisfying users' IT requirements, an organization's SDLC must include procedures to define information requirements; formulate alternative courses of action; perform technological, economic, and operational feasibility studies; and assess risks. These solutions should be consistent with the strategic IT plan, and the technology infrastructure and information architecture contained therein. At the completion of this process, an organization must decide what approach will be taken to satisfy users' requirements, and whether it will develop the IT solution in-house or will contract with third parties for all or part of the development.

IT Process 4: Develop and Acquire IT Solutions

After IT solutions have been identified and approval to proceed has been received, development and/or appropriate acquisition of the application (i.e., business process) software, infrastructure, and procedures may begin. Note: When discussing the actual computer software that is used to facilitate the execution of a given business process, we use the term *application software*. A given business process may use more than one application. For instance, a sales process might have one application for customer relationships, one for sales orders, and another for customer payments. In all likelihood, these applications would be linked to one another; nevertheless, they might actually represent three distinct applications.

Develop and Acquire Application Software

To ensure that applications will satisfy users' IT requirements, an organization's SDLC should include procedures to create design specifications for each new, or significantly modified, application and to verify those specifications against the user requirements. The specifications should be developed with systems users and approved by management and user departments. Design specifications include those for inputs, outputs, processes, programs, and stored data.

Acquire Technology Infrastructure

The SDLC should include procedures to ensure that platforms (hardware and systems software) support the new or modified application. Further, an assessment should be made of the impact of new hardware and software on the performance of the overall system. Finally, procedures should be in place to ensure that hardware and systems software are installed, maintained, and changed to continue to support business processes.

Develop Service Level Requirements and Application Documentation

ENTERPRISE SYSTEMS

E-BUSINESS

To ensure the ongoing, effective use of IT, the organization's *SDLC* should provide for the preparation and maintenance of service-level requirements and application documentation. *Service-level requirements* include such items as availability, reliability, performance, capacity for growth, levels of user support, disaster recovery, security, minimal system functionality, and service charges. These requirements become benchmarks for the ongoing operation of the system. As IT organizations become larger and more complex, especially those that must implement and operate enterprise systems, these service-level requirements become important methods for communicating the expectations of the business units for IT services. Further, if the organization is engaged in e-business, these service levels become benchmarks for service on a Web site or with business partners engaged in e-commerce.

The SDLC should include processes to ensure that comprehensive documentation is developed for each application to enable the effective use, operation, and maintenance of the application. *Application documentation* typically includes the following:

- *Systems documentation:* Provides an overall description of the application, including the system's purpose; an overview of system procedures; and sample source documents, outputs, and reports.
- *Program documentation:* Provides a description of an application program and usually includes the program's purpose; program flowcharts; source code listings; descriptions of inputs, data, and outputs; program test data and test results; and a history of program changes and approvals of such changes.
- *Operations run manual:* Gives detailed instructions to *computer operators* and to *data control* about a particular application. These manuals typically specify input source, form, and when received; output form and distribution; and computer operation instructions, including setup, required data, restart procedures, and error messages.
- *User manual:* Describes user procedures for an application. These instructions, which assist users in preparing inputs and using outputs, include a description of the application, procedures for completing source documents, instructions on how to input data to the computer, descriptions of manual files and computerized data, instructions on how to perform manual and automated processing, explanations of controls (including how to detect and correct errors), and procedures for distributing and using normal outputs.
- *Training material:* Helps users learn their jobs and perform consistently in those jobs.

IT Process 5: Integrate IT Solutions into Operational Processes

ENTERPRISE SYSTEMS

To ensure that a new or significantly revised system is suitable, the organization's SDLC should provide for a planned, tested, controlled, and approved conversion to the new system. As we noted at the start of the chapter, the testing conducted by Honeywell during development of the Boeing 777 flight control software had failed to detect a software bug that well might have led to a disastrous outcome had the pilot not been able to regain control of the aircraft. After installation, the SDLC should call for a review to determine that the new system has met users' needs in a cost-effective manner. When organizations implement enterprise systems, the successful integration of new information systems modules into existing information and operations processes becomes more difficult and more important. The challenges are the result of the interdependence of the business processes and the complexity of these processes and their connections. Any failure in a new system can have catastrophic results.

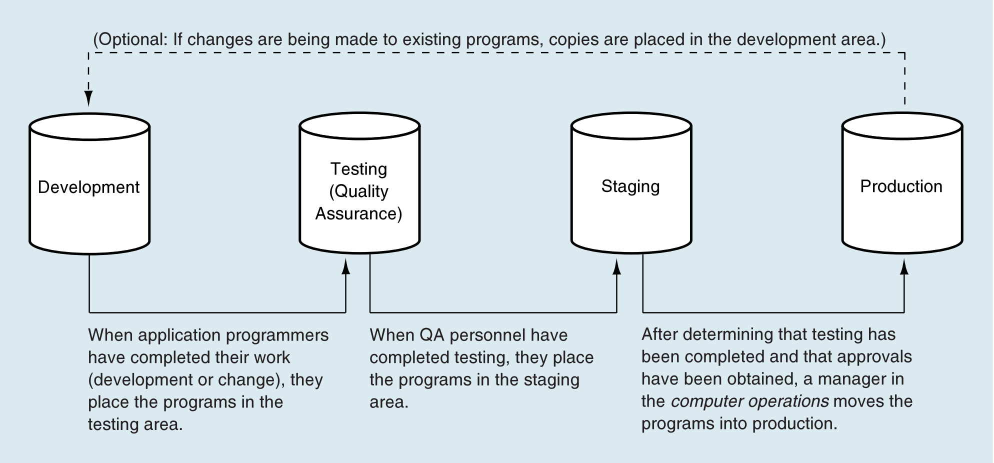
IT Process 6: Manage Changes to Existing IT Systems

To ensure processing integrity between versions of systems and to ensure consistency of results from period to period, changes to the IT infrastructure (hardware, systems software, and applications) must be managed via change request, impact assessment, documentation, authorization, release and distribution policies, and procedures.

ENTERPRISE SYSTEMS

Program change controls provide assurance that all modifications to programs are authorized and that the changes are completed, tested, and properly implemented. At

FIGURE 8.6 Illustration of Program Change Controls


(Optional: If changes are being made to existing programs, copies are placed in the development area.)
Development
Testing (Quality Assurance)
Staging
Production
When application programmers have completed their work (development or change), they place the programs in the testing area.
When QA personnel have completed testing, they place the programs in the staging area.
After determining that testing has been completed and that approvals have been obtained, a manager in the *computer operations* moves the programs into production.

the start of this chapter, we described the Trojan Horses planted on the computers of Amnon Jackont and 60 Israeli companies. Obviously, there were unauthorized changes that circumvented normal program change control procedures. Changes in documentation should mirror the changes made to the related programs. Figure 8.6 depicts the stages through which programs should progress to ensure that only authorized and tested programs are placed in production. Notice that separate organizational entities (see Figure 8.2, pg. 249) are responsible for each stage in the change process. These controls take on an even higher level of significance with enterprise systems. Should unauthorized or untested changes be made to such systems, the results could be disastrous. For example, assume that a change is made to the inventory module of an ERP system without testing to see the impact that change will have on the sales module used to enter customer orders. Because these two modules work together, and orders from customers for inventory cannot be processed without the inventory module, changes to either module must be carefully planned and executed.

Deliver and Support Domain

The Deliver and Support domain includes processes to deliver required IT services efficiently and effectively; ensure security and continuity of services; set up support services, including training; and ensure integrity of application data. Management wants to know that IT services are delivered in line with business priorities and in a cost-effective manner. Application programs and data must be available as needed, and the integrity and confidentiality of data must be maintained. Computing resources that are lost, destroyed, or unavailable for use can lead to lost revenues as well as increased costs to correct problems that may have occurred. Finally, unauthorized use of the computing resources can lead to fraud and sanctions or violations of laws and regulations, such as those related to privacy.

IT Process 7: Deliver Required IT Services

This process includes activities related to the delivery of the IT services that were planned by the IT processes in the Plan and Organize domain, and developed and implemented by the IT processes in the Acquire and Implement domain. Table 8.3 describes some of the key service-delivery activities.

TABLE 8.3 Delivering Required Services

Activity	Discussion
Define service levels	To ensure that internal and third-party IT services are effectively delivered, service-level requirements, for the minimum levels of the quantity and quality of IT services, must be defined.
Manage third-party services	To ensure that IT services delivered by third parties continue to satisfy organizational requirements, processes must be in place to identify, manage, and monitor nonentity IT resources.
Manage IT operations	To ensure that important IT functions are performed regularly and in an orderly fashion, standard procedures for IT operations must be established, including procedures for staff, job scheduling, and preventive maintenance.
Manage data	To ensure that data remain *complete, accurate,* and *valid,* management should establish a combination of application and general controls. *Application controls* relate directly to the data as it is being processed. *General controls* ensure data integrity after the data has been processed.
Identify and allocate costs	To ensure that IT resources are delivered in a cost-effective manner and that they are used wisely, management should identify the costs of providing IT services and should allocate those costs to the users of those services.

IT Process 8: Ensure Security and Continuous Service

In addition to managing ongoing IT operations, the IT function must see that IT services continue to be provided at the levels expected by the users. To do so, they must provide a secure operating environment for IT and plan for increases in required capacity and losses of usable resources. Capacity of all IT resources must be determined and managed, and resource modifications (increases or decreases) must be properly planned. To ensure that IT assets are not lost, altered, or used without authorization, management should establish a process to account for all IT components, including *applications* and *infrastructure*, and to prevent unauthorized alterations of assets or use of unauthorized assets. To ensure that barriers to efficient and effective use of the IT resource are prevented or eliminated and that the IT resource remains available, processes should be in place to identify, track, and resolve in a timely manner problems and incidents that occur. Three important aspects of the IT processes designed to address these issues are discussed in the following sections: ensuring continuous service, restricting access to computing resources, and ensuring physical security.

Ensure Continuous Service

To ensure that sufficient IT resources continue to be available for use in the event of a service disruption, management should establish a process, coordinated with the overall business continuity strategy, which includes business continuity or contingency planning as well as disaster recovery planning for all IT resources and related business resources, both internal and external. These control plans are directed at potential calamitous losses of resources or disruptions of business processes, for both the organization and its business partners, which could imperil the organization's very survival. Catastrophes like Hurricanes Katrina and Rita in 2005; earthquakes in Los Angeles and San Francisco; terrorist attacks on the World Trade Center and the Pentagon in 2001; dockworker strikes that can leave hundreds of ships with no place to unload their goods; and power outages, such as the Great Northeast Power Blackout of 2003, have struck fear in the hearts of many executives that their firms might be brought to their knees by natural or man-made disasters. **Business continuity planning** (also known as **disaster recovery planning**, **contingency planning**, and **business interruption planning**) is a process that identifies events that may threaten an organization and provides a framework to ensure that the organization will continue to operate when the threatened event occurs, or will resume operations with a minimum of disruption.

A number of business continuity planning models are available. The following are the six stages reflected in a business continuity management lifecycle model developed by the Business Continuity Institute.[13] Think about a wagon wheel, with a center hub and five spokes. The first element, the business continuity management program, serves as the hub that glues the entire business continuity lifecycle together.

1. *Establish a formal business continuity management program (the hub of the wheel previously described):* Gain the approval and *proactive* participation of the board of directors; define roles, accountability, responsibility, and authority; determine necessary levels of finances and resources; develop metrics, scorecards, and/or benchmarks for evaluating the effectiveness and efficiency of the program.
2. *Understand your business:* Conduct a business impact analysis and risk assessment to determine the probability and impact of specific threats that could disrupt key business processes.
3. *Create business continuity strategies:* Design continuity and recovery strategies for the entire organization and all business processes.
4. *Develop and implement a business continuity response:* Formalize a response plan; determine how to define and handle crises and incidents; and create incident response teams and related communication networks.
5. *Build and embed a business continuity management culture in the organization:* Engage in ongoing programs of education, awareness, and training.
6. *Maintain and audit the business continuity plan:* Rehearse the plan with affected parties, test the technology and other business continuity systems, and continually maintain and update the plans. Remember, business continuity planning reflects an ongoing process.

E-BUSINESS

For our discussions here, we want to focus on those elements of business continuity planning that relate to business processes, especially those supported by IT. But, let's not lose sight of the fact that business continuity management reaches beyond IT to providing continuity planning for resources (e.g., people, supplies, documentation) residing in operational business units of the organization. Also, the plan may extend beyond the organization for key resources provided by third parties. You also might note that the current thinking is that we should plan contingencies for important *processes* rather than individual *resources*. Thus, we would develop a contingency plan for our Internet presence, rather than for our Web servers, networks, and other related resources that enable that presence.

In the remainder of this section, we describe the major strategies that are used to provide for the continuity of IT services. Two major elements are required. First, we must have alternative computer facilities and related resources (e.g., electricity, personnel, and communications) that can be used should the primary facilities and resources become unavailable. Second, we must have the programs, data, and documentation necessary to continue or resume operations. The strategy chosen for one often coincides with the strategy for the other. In the simplest of cases, we *periodically* make a copy of important stored data, programs, and documentation. These copies are

[13] "The Business Continuity Institute, Good Practice Guidelines (2005): A Framework for Business Continuity Management," Available, as of June 2006, at *http://www.thebci.org*.

called **backups**, and they would typically be stored in a secure location not located near the primary facility. Data files are often backed up to tapes or disks and may be picked up by and stored at third-party facilities such as those operated by Iron Mountain, Inc. and SunGard. When a disaster occurs, the backups are moved to sites where the organization can again resume processing. At the beginning of the chapter, we described the problems that SCP Pool Corp. encountered when they tried to recover backups from an Iron Mountain facility. The process whereby we restore the lost data and resume operations is called **recovery**. The recovery need not be at an alterative site. Data might be lost or destroyed at a primary site that remains available for use. In this case, we use the backup data to restore the lost data and to resume operations. In general, such procedures are called "backup and recovery."

E-BUSINESS

Some organizations, especially organizations such as airlines and those with significant e-business operations, need to keep their systems and Internet commerce sites online at all times and cannot tolerate any break in operations, or must have instant recovery from an interruption; a typical backup and recovery process will not do the job for these organizations. Even more traditional organizations cannot operate for extended periods of time without their IT operations; they cannot manufacture goods, accept customer orders, or order raw materials. All organizations must perform a risk assessment to determine the likelihood that their systems will become unavailable, the losses that could result, and the costs they are willing to incur to address the risks.

Organizations that must ensure continuous operations may maintain and operate two or more sites (e.g., SCP Pool Corp maintained facilities in Dallas, TX and Covington, LA), each containing identical equipment and identical copies of all programs, data, and documentation. Should the primary facility become unavailable, one of the secondary sites takes over, sometimes automatically and without noticeable delay. In these situations, data must be replicated in real-time on primary and secondary systems. This data replication strategy is called **Continuous Data Protection (CDP)** whereby all data changes are data stamped and saved to secondary systems as the changes are happening on the primary. Notice that this process is not the periodic backup of files mentioned previously but is a process for continuous and immediate replication of any data changes. The site that maintains copies of the primary site's programs and data is a **mirror site**.

E-BUSINESS

An organization unwilling (e.g., not cost effective) to maintain duplicate computer facilities but still needing CDP might contract with third parties such as U.S. Data Trust Corporation or Iron Mountain, Inc. for **electronic vaulting**, a service whereby data changes are automatically transmitted over the Internet on a continuous basis to an off-site server maintained by the third party. When needed, the backed up data can be retrieved from the electronic vault to recover from a data loss at the primary computer facility or to resume interrupted operations on an alternative facility. For those companies not maintaining the duplicate computer facilities, a good control strategy is to make arrangements with hardware vendors, service centers, or others for the standby use of compatible computer equipment. These arrangements are generally of two types—*hot sites* or *cold sites*.

A **hot site** is a fully equipped data center, often housed in bunker-like facilities, that can accommodate many businesses and that is made available to client companies for a monthly subscriber fee. Less costly, but obviously less responsive, is a **cold site**. A cold site is a facility usually comprised of air-conditioned space with a raised floor, telephone connections, and computer ports into which a subscriber can move equipment. The disaster recovery contractor or the manufacturer provides the necessary equipment. Obviously, it is necessary to have a contract for the delivery of the replacement equipment to ensure that it will be available when needed. A company that contracts for either a hot site or a cold site should expect some delay in getting operations up and

Technology Summary 8.1

DENIAL-OF-SERVICE ATTACKS

In a **denial-of-service attack**, a Web site is overwhelmed by an intentional onslaught of thousands of simultaneous messages, making it impossible for the attacked site to engage in its normal activities. A **distributed denial-of-service attack** uses many computers (called *zombies,* see Technology Summary 7.4 on pg. 224 in Chapter 7) that unwittingly cooperate in a *denial-of-service attack* by sending messages to the target Web sites. Unfortunately, the distributed version is more effective because the number of computers responding multiplies the number of attack messages. And, because each computer has its own IP address, it is more difficult to detect that an attack is taking place than it would be if all the messages were coming from one address. Denial-of-service attacks can be categorized into four levels, with progressively more severe consequences: (1) inundating the server with bogus requests; (2) consuming CPU cycles, memory, and other resources; (3) disabling Web traffic by misconfiguring routers; and (4) sending mail-bombs to individuals, lists, or domains.

Currently, no easy *preventive* controls exist. To *detect* a denial-of-service attack, Web sites may employ *filters* to sense the multiple messages and block traffic from the sites sending them, and *switches* to move their legitimate traffic to servers and Internet service providers (ISPs) that are not under attack (i.e., *corrective*). However, attackers can hide their identity by creating false IP addresses for *each* message, making many filtering defenses slow to respond or virtually ineffective. An organization might also carry insurance to reimburse it for any losses suffered from an attack (i.e., *corrective*).

running after a disaster strikes as, at a minimum, it must relocate operations to that site. In the aftermath of Hurricane Katrina, some organizations found hot sites got very heavy usage because so many firms had simultaneously declared disasters.

E-Business

We conclude this section with a discussion of a serious threat that can affect the capability of Internet-based businesses such as eBay and Amazon.com to ensure continuous service to their customers. Technology Summary 8.1 describes this phenomenon, *denial-of-service attacks*, and the processes that might be put in place to detect and correct them to ensure that organizations achieve the level of service that they plan.

Restrict Access to Computing Resources

At the beginning of the chapter, we described how an employee at Progressive Casualty Insurance had obtained, and misused, data to which she was not authorized access. Other such unauthorized disclosures have been reported. For example, a laptop belonging to Fidelity Investments was stolen that contained the personal information, including social security numbers, of 196,000 current and former Hewlett-Packard, Co. employees. Another laptop, this one belonging to an employee of Ameriprise Financial Inc., was stolen that contained the names and account numbers of 158,000 Ameriprise clients and the names and social security numbers of 67,000 current and former financial advisors.[14] Yet another laptop, this one belonging to an employee of Ernst & Young, was stolen. This laptop contained the names and credit card numbers of about 243,000 Hotels.com customers.[15] Finally, lest you think that laptops are the only problem, ABN Amro Mortgage Group, Inc. reported that some data tapes that were in transit to its credit-reporting bureau were lost in transit. These tapes contained the personal information on

[14] Jennifer Levitz and John Hechinger, "Laptops Prove Weakest Link in Data Security," *The Wall Street Journal*, March 24, 2006, pp. B1, B2.

[15] David Reilly, "Hotels.com Credit-Card Data Lost in Stolen Laptop Computer; Machine Taken from Car of Ernst & Young Worker; Theft Appears to Be Random," *The Wall Street Journal*, June 2, 2006, p. A14.

more than 2 million customers.[16] The companies losing this personal data have often provided one year of credit monitoring service, by companies such as Equifax, TransUnion, and Experian, to reduce the possibility that the lost personal data will be used to perform fraudulent activities.

What's the problem here? Management has a legal responsibility to protect an organization's assets, including informational assets. For example, the unauthorized disclosure of financial information (i.e., nonpublic data) is a violation of federal securities laws. Also, various laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 places restrictions on the use, handling, and disclosure of individually identifiable health information. To ensure that organizational information is not subjected to unauthorized use, disclosure, modification, damage, or loss, management should implement logical and physical access controls to ensure that access to computing resources—systems, data, and programs—is restricted to authorized users for authorized uses by implementing two types of plans:

- Control plans that restrict physical access to computer facilities
- Control plans that restrict logical access to stored programs, data, and documentation

E-BUSINESS

Figure 8.7 shows the levels (or layers) of protection included in each of these categories. Use Figure 8.7 as a road map to the discussion that follows. As you study this section, consider how much more important these controls become when the organization engages in e-business and has electronic connections to customers and business partners.

Control Plans for Restricting Physical Access to Computer Facilities. Naturally, only authorized personnel should be allowed access to the computer facility. As shown in Figure 8.7, control plans for restricting physical access to computer facilities encompass three layers of controls.

One important type of control is the **biometric identification system**. Although not foolproof, the technology has improved dramatically in recent years, leading to the widening use of such systems in practice. The most common biometric devices are those that read fingerprints. In fact, biometric fingerprint identification is used to secure physical access to many types of facilities and devices such as laptops and PDAs. For example, Deutsche Bank AG in Frankfurt and Citibank in New York have for years been using biometrics for employee access to computer server rooms.[17] Another example can be found at the London City Airport, where they use fingerprint identification to control access to its secure areas for 1,600 employees.[18] Although controls for restricting physical access to computer facilities seem straightforward and are generally accepted as good practice, they are not always effectively implemented. Some of the security lapses uncovered by security consulting firms include the following:[19]

- Metal detectors at a front entrance that can be bypassed by taking a series of elevators and hallways to an unguarded door
- Unlocked doors to computer rooms and utility rooms housing electrical connections and network wiring

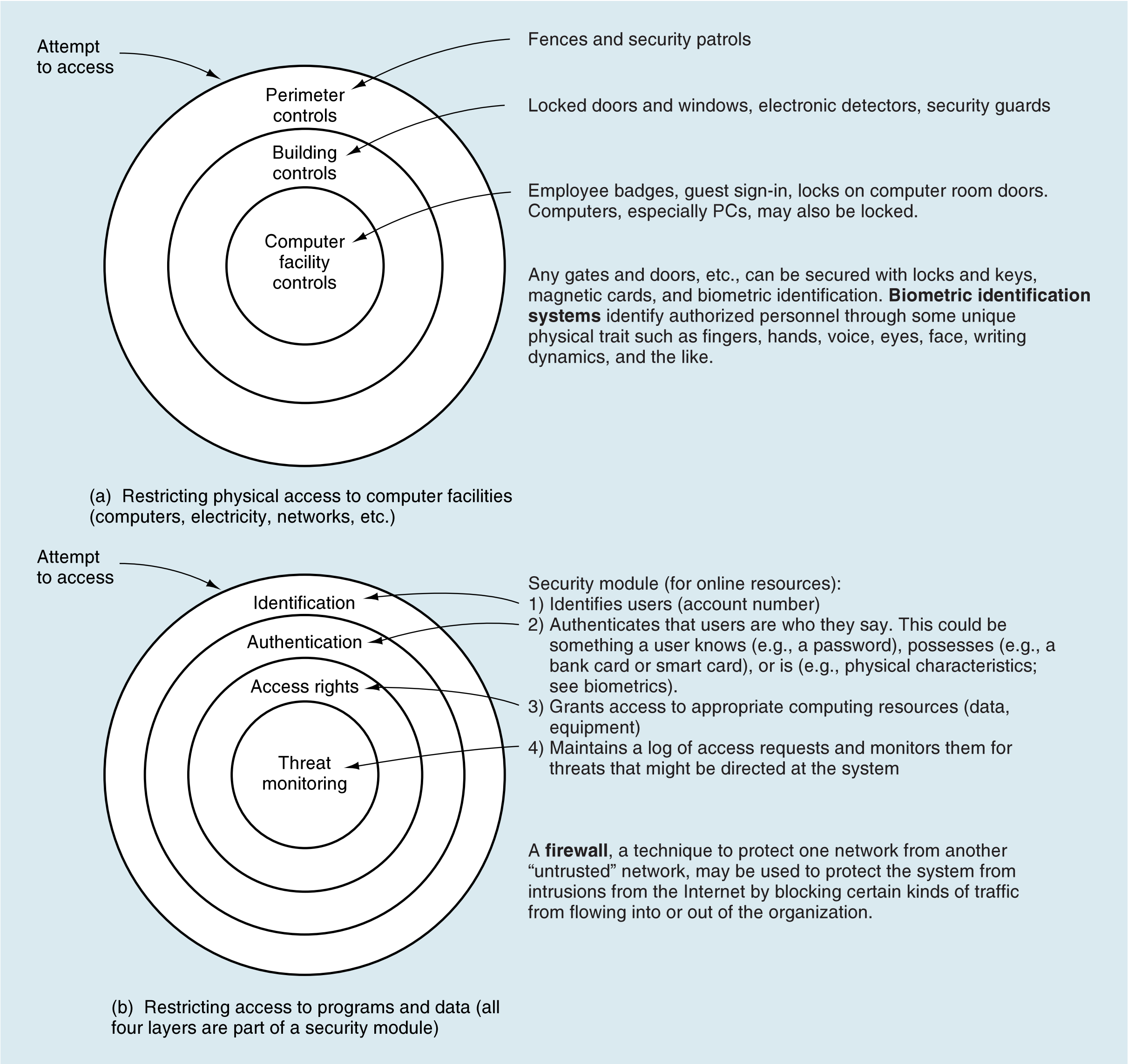
[16] Lucas Mearian, "ABN Amro Unit Reveals Electronic Data-Transfer Plan After Tape Snafu," *Computerworld*, January 2, 2006, p. 6.

[17] Lucas Mearian, "Banks Eye Biometrics to Deter Consumer Fraud," *Computerworld*, January 28, 2002, p. 12.

[18] "Airport Rolls Out Biometric Security," CNN, *http://www.cnn.com/2003/WORLD/europe/05/27/biz.trav.biometric.airport/index.html*, May 27, 2003 (story available as of June 2006).

[19] Robert L. Scheier, "Lock the Damned Door!" *Computerworld* (February 10, 1997): 66–68.

FIGURE 8.7 Restricting Access to Computing Resources—Layers of Protection



Fences and security patrols

Locked doors and windows, electronic detectors, security guards

Employee badges, guest sign-in, locks on computer room doors. Computers, especially PCs, may also be locked.

Any gates and doors, etc., can be secured with locks and keys, magnetic cards, and biometric identification. **Biometric identification systems** identify authorized personnel through some unique physical trait such as fingers, hands, voice, eyes, face, writing dynamics, and the like.

(a) Restricting physical access to computer facilities (computers, electricity, networks, etc.)

Security module (for online resources):
1) Identifies users (account number)
2) Authenticates that users are who they say. This could be something a user knows (e.g., a password), possesses (e.g., a bank card or smart card), or is (e.g., physical characteristics; see biometrics).
3) Grants access to appropriate computing resources (data, equipment)
4) Maintains a log of access requests and monitors them for threats that might be directed at the system

A **firewall**, a technique to protect one network from another "untrusted" network, may be used to protect the system from intrusions from the Internet by blocking certain kinds of traffic from flowing into or out of the organization.

(b) Restricting access to programs and data (all four layers are part of a security module)

- Sensitive files, containing telephone numbers, passwords, confidential information, and so on, lying out on desks in unsecured areas
- Unrestricted access to devices that are printing confidential information

Control Plans for Restricting Logical Access to Stored Programs, Data, and Documentation. Control plans for restricting logical access to stored programs, data, and documentation entail a number of techniques aimed at controlling *online* and *offline* systems. In an online environment, access control software called the **security module** will (1) ensure that only authorized users gain access to a system through a process of *identification* (e.g., a unique account number for each user) and *authentication* (e.g., a password to verify that the user is who they say they are), (2) associate with authorized users the computing resources they are permitted to access and the action privileges (e.g., read, copy, write data) they have with respect to those resources (*access rights*), and (3) report violation attempts. These steps are depicted in part (b) of Figure 8.7 (pg. 269).

Passwords are a notoriously weak method for authenticating user identification. Because people often have many passwords, they create ones that are easy to remember (and therefore easy to guess), or they write them down. In either case, someone intent on getting access to a system could easily obtain such passwords. Faced with the weakness of passwords, many organizations are using biometrics to authenticate user identification. For example, the IT staff at Telesis Community Credit Union ran a network password cracker to see if employees were adhering to Telesis' password policies. Within 30 seconds, the cracker program had identified 80 percent of user passwords. After asking employees to create stronger passwords, the cracker program detected 70 percent of passwords. Telesis concluded that the use of strong passwords was just not going to happen and installed a fingerprint system to authenticate users.[20] To strengthen security systems even further and reduce the incidences of identify theft, many organizations employ two-factor authentication strategies, which require users to verify their identity by two means, such as a bank card and a PIN or biometric identification and a password.

To prevent unauthorized access to computer networks, organizations use a **firewall** (see Figure 8.7 on pg. 269) to block all traffic except that which is explicitly authorized. After a user has accessed a network, the *threat-monitoring* portion of the security module may employ an **intrusion-detection system (IDS)** to monitor system and network resources and activities and "learn" how users typically behave on the system. The typical behavior is accumulated in *user profiles*. Subsequently, when usage patterns differ from the normal profile, the exceptional activity is flagged and reported. IDSs can be used to detect attacks from outside the organization, such as *denial-of-service attacks*, or from inside the organization, as when authorized users attempt to undertake unauthorized actions. Organizations not wanting to wait until an authorized activity *has* occurred might employ an **intrusion-prevention system (IPS)** to actively block unauthorized traffic using rules specified by the organization.

The primary plans for restricting access in an *offline* environment involve the use of segregation of duties, restricting physical access to computer facilities, program change controls, and library controls. The first three plans have been defined and discussed in previous sections. **Library controls** restrict access to data, programs, and documentation. Library controls are provided by a *librarian function*, a combination of people, procedures, and computer software that serves two major purposes. First, library controls limit the use of stored data, programs, and documentation to authenticated users with authorized requests. Second, they maintain the storage media (e.g., disks, tapes).

In *online* environments, librarian software is used to restrict access to online programs, data, and documentation. For example, the software will keep track of the many versions of event and master data and ensure that the latest versions of such data are used. The software can also permit appropriate access to development, testing, staging, and production versions of programs (refer to Figure 8.6, pg. 263).

Before we leave this section, let's explore a topic that always receives much media attention, *computer hacking*. We discuss this topic in Technology Summary 8.2. Interestingly, some security companies are hiring young, technology-savvy teenagers to try to break into clients' computer systems to find weaknesses. These bands of "white hat" hackers are let loose in an "information security sandbox" to determine vulnerable spots

[20] Kym Gilhooly, "Biometrics: Back to Basics," *Computerworld* (May 9, 2005): 19–20.

Technology Summary 8.2

COMPUTER HACKERS AND CRACKERS

In simple terms, **computer hacking and cracking** reflects the intentional, unauthorized access to an organization's computer system, accomplished by bypassing the system's access security controls. You can think of these acts as illegal breaking and entering. Usually, but not always, a person outside the organization does the hacking or cracking. A hacker is someone who gets a kick out of knowing the ''ins and outs'' of a computer system. Generally, hackers do not hold malicious intentions to destroy or steal; rather, they feel clever, powerful, and proud of their hacking successes. They enjoy building sought-after reputations among the underground world of hackers. On the other hand, whereas crackers employ many of the same penetration techniques as hackers, they do so with sinister motives that are bent on crime, theft, and destruction. However, as benign as hackers like to think they are, their illegal attempts to gain access into the computers and networks of others can result in serious damage and unwanted personal consequences. One renowned case of a so-called benign-motive type of hacking occurred in 1988 when a Cornell University graduate student infiltrated the Internet and planted a virus that he thought would not be destructive. However, it proved to be extremely so. It crashed some 6,000 computers on that network; as a result, the student gained more notoriety by becoming the first person charged with violating the Federal Computer Fraud and Abuse Act.

Hackers/crackers take a variety of steps to get the information they need to bypass security modules and firewalls—some ploys are ingenious, others mundane. Some of them merely ''schmooze'' unsuspecting employees to learn passwords.[a] This technique might work as follows.

The hacker/cracker will call the ''target'' and claim that it appears that the ''target'' is trying to break into a key system—say accounting. The ''target'' will deny it vehemently, and when the panicked ''target'' thinks he or she is in real trouble, the hacker will ask, ''Well, then, what user name are you using now?'' The ''target'' will give his or her user name. Then, the hacker/cracker finishes it off with, ''Well, then you are using the wrong password with that account. Are you using the new password?'' The ''target'' will respond, ''What new password?'' Then the hacker/cracker will say, ''Oh great! Now this is really messed up! What password are you using?'' The ''target'' then gives up his or her password.[b]

Others employ ''dumpster diving,'' searching through rubbish for system information such as passwords.[c] Some use ''sniffer'' programs that travel over telephone lines gathering passwords. Still others simply try to log on to a system by using commonly used passwords. Some of these techniques are now being used by businesses engaged in counter-hacking/cracking, known also as *penetration testing*. Clients hire these companies, including at least one Big Four accounting firm, to test the clients' computer systems for security weaknesses by attempting to legally hack their way into those systems.

Note:

[a] One security expert reports that a third of the computer crime cases that he has investigated involved an individual who had been talked out of a critical password. ''Cyber Crime,'' *Business Week* (February 21, 2000): 42.

[b] ''Securing the Network: Data Security Essentials,'' *Getting Results* (March 1997): 5.

[c] A case in point concerned a New York telephone company that sent a promotional letter to calling card customers, with PIN numbers printed on the letter. Dumpster divers scrambled for the discarded letters.

in computers and networks: "Fortified by pizza and soda, they [study] a computer systems weaknesses looking for ways to break in and steal information."[21]

Ensure Physical Security

To protect the IT facilities against man-made and natural hazards, the organization must install and regularly review suitable environmental and physical controls. These plans reduce losses caused by a variety of physical, mechanical, and environmental

[21] "Enlisting the Young as White Hat Hackers," *The New York Times* (May 29, 2003).

TABLE 8.4 Environmental Controls

Environmental Hazard	Controls
Fire	Smoke detectors, fire alarms, fire extinguishers, fire-resistant construction materials, insurance
Water damage	Waterproof ceilings, walls, and floors; adequate drainage; water and moisture detection alarms; insurance
Dust, coffee, tea, soft drinks	Regular cleaning of rooms and equipment, dust-collecting rugs at entrances, separate dust-generating activities from computer, do not allow food/drink near computers, good housekeeping
Energy increase, decrease, loss	Voltage regulators, backup batteries and generators

events. Fire and water damages represent major threats to most businesses, as do power outages and lax data backup procedures. Table 8.4 summarizes some of the more common controls directed at these environmental hazards.

The advanced state of today's hardware technology results in a high degree of equipment reliability; unless the system is quite old, hardware malfunctions are rare. Even if a malfunction occurs, it is usually detected and corrected automatically. In addition to relying on the controls contained within the computer hardware, organizations should perform regular **preventive maintenance** (periodic cleaning, testing, and adjusting of computer equipment) to ensure its continued efficient and correct operation.

IT Process 9: Provide Support Services

To ensure that users make effective use of IT, management should identify the training needs of all personnel, internal and external, who make use of the organization's IT services, and should see that timely training sessions are conducted. To effectively use IT resources, users often require advice and may require assistance to overcome problems encountered in using those resources. This assistance is generally delivered via a "help desk" function.

Monitor and Evaluate Domain

Within the Monitor and Evaluate domain is a process to assess IT services for quality and to ensure compliance with control requirements. Monitoring may be performed as a self-assessment activity within IT, by an entity's internal/IT audit group, or by an external organization such as a public accounting firm. Without the feedback provided by the monitoring process, the system of internal control is not complete.

IT Process 10: Monitor and Evaluate the Processes

To ensure the achievement of IT process objectives, management should establish a system for defining performance indicators (service levels), gathering data about all processes, and generating performance reports. Management should review these reports to measure progress toward identified goals. To increase confidence that IT objectives are being achieved and that controls are in place, and to benefit from advice regarding best practices for IT, independent audits should be conducted on a regular basis.

E-BUSINESS

As previously mentioned in Chapter 1, the American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants have developed a set of professional assurance and advisory services based on a common set of Trust Service

TABLE 8.5 Trust Services Principles

Principle	Description
Security	Determines whether the system is protected against unauthorized access (both physical and logical)
Availability	Determines whether the system is available for operation and use as committed or agreed
Processing Integrity	Determines whether processing is complete, accurate, timely, and authorized
Online Privacy	Determines whether private information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed
Confidentiality	Determines whether business information designated as confidential is protected as committed or agreed

Source: ''Suitable Trust Services Criteria and Illustrations for Security, Availability, Processing Integrity, Online Privacy, and Confidentiality (Including WebTrust® and SysTrust®),'' http://www.aicpa.org. Copyright © 2003 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants.

principles, which are outlined in Table 8.5. These principles apply to WebTrust® and SysTrust® engagements, among others.

The WebTrust® (version 3.0) family of services offers best practices and e-business solutions related to business-to-consumer and business-to-business electronic commerce. Some of the services within the family include WebTrust® Confidentiality, WebTrust® Online Privacy, and WebTrust® Consumer Protection.

SysTrust® (version 2.0) is an assurance service designed to test and monitor the reliability of an entity's information system and databases, including ERP systems.

As you can see, the accounting profession is very involved with not only the Monitor and Evaluate domain (refer to Figure 8.3 on pg. 251), but also the Plan and Organize, Acquire and Implement, and Deliver and Support domains outlined in the COBIT framework.[22]

Summary

In this chapter, we discussed the problems inherent in controlling the activities of the IT function. We suggested some controls that can help reduce IT risks and take advantage of opportunities for strategic implementation of emerging information technology. To put these IT processes/control plans into perspective once again, return to the hierarchy shown in Figure 7.3 (pg. 219). Note that pervasive control plans, including the IT general controls/IT processes discussed in this chapter, provide a second umbrella of protection, in addition to the control environment, over all AIS business processes. In Chapter 9, we will begin to examine the third level in the hierarchy, business process control plans and application controls, by looking at those controls associated with the technology used to implement a business process. Then, in Chapters 10 through 15, we continue the coverage of the business process control plans and application controls by examining those related to each specific business process.

[22] These services are introduced in Chapter 1.

Key Terms

IT governance
segregation of duties
security officer
IT steering committee
rotation of duties
forced vacations
fidelity bond
systems development life cycle (SDLC)
program change controls
business continuity planning
disaster recovery planning
contingency planning
business interruption planning
backup
recovery
Continuous Data Protection (CDP)
mirror site
electronic vaulting
hot site
cold site
denial-of-service attack
distributed denial-of-service attack
biometric identification systems
security module
firewall
intrusion detection systems (IDS)
intrusion prevention systems (IPS)
library controls
computer hacking and cracking
preventive maintenance

Review Questions

RQ 8-1 What is IT governance?

RQ 8-2 What is the difference among a pervasive control plan, a general control, a business process control, an application control, and an IT control process?

RQ 8-3 Name and describe the four IT resources.

RQ 8-4 How does the COBIT framework define control?

RQ 8-5 What are the principal responsibilities, major duties, and key control concerns of *each* functional position pictured in Figure 8.2 on pg. 249 (i.e., the organization chart of an IT organization)?

RQ 8-6 What are the four IT control process domains?

RQ 8-7 What is the purpose of the strategic IT plan?

RQ 8-8 What are the major elements of the strategic IT plan?

RQ 8-9 Segregation of duties consists of separating what four basic functions? Briefly define each function.

RQ 8-10 Describe some compensating controls that can be used to reduce exposures when it is not possible to properly segregate duties in a small organization.

RQ 8-11 How can the consolidation of functions within IT *increase* internal control?

RQ 8-12 What functions within the IT organization should be segregated?

RQ 8-13 What is the function of the security officer?

RQ 8-14 What is the function of the IT steering committee?

RQ 8-15 Describe personnel control plans.

RQ 8-16 What is the systems development life cycle (SDLC)?

RQ 8-17 What types of documentation constitute a well-documented application? Describe each type.

RQ 8-18 Name and describe the four IT control processes in the Acquire and Implement domain.

RQ 8-19 What are the four stages through which a program should move as it is being developed? Who should have responsibility for each of those phases?

RQ 8-20 What steps are commonly included in a business continuity planning methodology?

RQ 8-21 Describe backup and recovery.

RQ 8-22 Describe continuous data protection (CDP), a mirror site, and electronic vaulting.

RQ 8-23 What is the difference between a *hot site* and a *cold site*?

RQ 8-24 Describe a *denial-of-service attack*. What controls are recommended to detect or correct such an attack?

RQ 8-25 Describe the three layers of controls for restricting physical access to computer facilities.

RQ 8-26 Explain *biometric identification systems*.

RQ 8-27 Describe the four layers of controls for restricting logical access to stored programs, data, and documentation.

RQ 8-28 Distinguish *firewalls, intrusion detections systems (IDS),* and *intrusion prevention systems (IPS).*

RQ 8-29 Describe *library controls*.

RQ 8-30 Define computer *hacking* and *cracking*, and explain how they undermine resource security.

RQ 8-31 a. What *kinds* of damage are included in the category of environmental hazards?

b. What control plans are designed to *prevent* such hazards from occurring?

c. What control plans are designed to *limit losses* resulting from such hazards or to recover from such hazards?

RQ 8-32 a. Why should an organization conduct monitoring activities?

b. Who might conduct monitoring activities?

Discussion Questions

DQ 8-1 ‘‘The Enterprise Risk Management (ERM) framework introduced in Chapter 7 can be used by management to make decisions on which controls in this chapter should be implemented.’’ Do you agree? Discuss fully.

DQ 8-2 Compare and contrast the COBIT definition of control in this chapter (pg. 247) with definitions in Chapter 7 for ERM (pg. 208), the COSO definition of internal control (pg. 216), and this textbook’s definition of internal control (pg. 219).

DQ 8-3 A key control concern described in Table 8.1 (pg. 250) regarding the systems development manager is that ‘‘systems development can develop and implement systems without management approval.’’ Discuss a control described in this chapter that reduces the risk that unauthorized systems will be implemented.

DQ 8-4 ‘‘The information systems function of *database administrator* is really a ‘two-edged sword.’ It presents the organization with both control problems and opportunities to tighten control.’’ Explain fully.

DQ 8-5 ‘‘In small companies with few employees, it is virtually impossible to implement the *segregation of duties* control plan.’’ Do you agree? Discuss fully.

DQ 8-6 ‘‘No matter how sophisticated a system of internal control is, its success ultimately requires that you place your trust in certain key personnel.’’ Do you agree? Discuss fully.

DQ 8-7 Debate the following point. ''*Business continuity planning* is really an IT issue.''

DQ 8-8 ''Contracting for a *hot site* is too cost-prohibitive except in the rarest of circumstances. Therefore, the vast majority of companies should think in terms of providing for a *cold site* at most.'' Discuss fully.

DQ 8-9 What *qualities of information* Exhibit 1.2 on pg. 20 in (see Chapter 1) might an organization fail to attain as a result of a *denial-of-service* attack? For each, describe a possible control.

DQ 8-10 ''Preventing the unauthorized disclosure and loss of data has become almost impossible. Employees and others can use iPods, flash drives, cameras, and PDAs, such as Blackberries and Treos, to download data and remove it from an organization's premises.'' Do you agree? Describe some controls from this chapter that might be applied to reduce the risk of data disclosure and loss for these devices.

DQ 8-11 ''The Monitor and Evaluate the Processes activity (IT process 10) must be performed by an independent function such as a CPA.'' Do you agree? Discuss fully.

DQ 8-12 Your boss was heard to say, ''If we implemented every control plan discussed in this chapter, we'd never get any work done around here.'' Do you agree? Discuss fully.

PROBLEMS

P 8-1 The following is a list of 12 control plans from this chapter.

Control Plans

A. Service level agreements

B. Firewall

C. Library controls

D. Security guards

E. User manuals

F. Security module

G. Personnel termination control plans

H. Biometric identification systems

I. Personnel selection and hiring control plans

J. Rotation of duties and forced vacations

K. Program change controls

L. Continuous data protection

The following is a list of 10 situations that have control implications.

Control Situations

1. During a violent electrical storm, an employee at Wendell Company was keying data at one of the computers in the order entry department. After about an hour of data entry, lightning caused a company-wide power failure. When power was restored, the employee had to rekey all the data from scratch.

2. The accounts payable department at Thornton Company did not have detailed instructions for completing the input form for approved vendor invoices. All the invoices added to the accounts payable master data for the last month lacked the field for ''due date.'' As a result, several

invoices were paid late, and Thornton lost cash discounts on several other vendor payments.

3. Tony and Fred have been friends for many years. Tony works in the shipping department at Torrington Company, an electronic wholesaler, and Fred is unemployed. To make a little money, Fred convinced Tony to lend him his employee badge (it has a magnetic strip on the back to open doors at Torrington Company), and Fred used the badge to access the Torrington warehouse and steal some electronics gear.

4. The customer service representatives at Sell-All, a catalog sales company, have been complaining that the computer system response time is very slow. They find themselves apologizing to customers who are waiting on the phone for their orders to be completed.

5. At Darrell Company, most transaction processing is automated. When an inventory item reaches its reorder point, the computer automatically prints a purchase order for the economic order quantity (EOQ). A programmer, who was in collusion with Deuce, Inc., the vendor that supplied several parts, altered the computer program and the inventory master data for those parts. He reduced the EOQ and made certain program alterations, so that items supplied by Deuce were ordered more often than Darrell required them.

6. The résumé of an applicant for the job of controller at Wilbur's Mills showed that the candidate had graduated, some 10 years earlier, magna cum laude from Enormous State University (ESU) with a major in accounting. ESU's accounting program was well respected, and Wilbur's Mills had hired several ESU graduates over the years. In his second month on the job, the new controller became tongue-tied when the chief financial officer (CFO) asked him a technical question about earnings per share reporting. When later it was discovered that the controller's degree from ESU was in mechanical engineering, he was dismissed.

7. June Cleaver, the company cashier, was known throughout the company as a workaholic. After three years on the job, June suddenly suffered a gall bladder attack and was incapacitated for several weeks. While she was ill, the treasurer temporarily assumed the cashier's duties and discovered that June had misappropriated several thousand dollars since she was hired.

8. A hacker accessed the Web site at Axcel, Inc. and changed some of the graphics. Confused by these changes, some customers took their business elsewhere.

9. During a normal workday, Tom, who was not an employee, entered Butternut Company's offices and was able to find and remove some computer printouts containing user IDs and other sensitive information. He later used that information to gain access to Butternut's computer system.

10. John is employed in the personnel department at Albany Company. From the computer in his office, John was able to access the order entry system at Albany and entered some orders for goods to be shipped to his cousin.

Match the 10 situations with a control plan that would *best* prevent the system failure from occurring. Because there are 12 control plans, you should have 2 letters left over.

P 8-2 Listed here are several control plans discussed in the chapter. On the blank line to the left of each control plan, insert a P (preventive), D (detective), or C (corrective) to classify that control most accurately. If you think that more than one code could apply to a particular plan, insert all appropriate codes and briefly explain your answer:

Code	Control Plan
_____ 1.	Library controls
_____ 2.	Program change controls
_____ 3.	Fire and water alarms
_____ 4.	Fire and water insurance
_____ 5.	Install batteries to provide backup for temporary loss in power
_____ 6.	Backup and recovery procedures
_____ 7.	Service level agreements
_____ 8.	IT steering committee
_____ 9.	Security officer
_____ 10.	Operations run manuals
_____ 11.	Rotation of duties and forced vacations
_____ 12.	Fidelity bonding
_____ 13.	Personnel management (supervision)
_____ 14.	Personnel termination procedures
_____ 15.	Segregation of duties
_____ 16.	Strategic IT plan
_____ 17.	Disaster recovery planning
_____ 18.	Restrict entry to the computer facility through the use of employee badges, guest sign-in, and locks on computer room doors.
_____ 19.	Computer security module
_____ 20.	Personnel development controls

P 8-3 Examine the last column in Table 8.1 (pg. 250) for the following personnel only: security officer, chief information officer, systems development manager, quality assurance, and systems programming.

For each of the five functions, list *one* control plan from this chapter that would address the control concern described in the last column of Table 8.1 for that function. Explain how the plan might address the concern mentioned. Do not use the same plan twice; use five different plans.

P 8-4 The following is a list of 12 control plans from this chapter.

Control Plans

A. Firewall

B. Backup batteries and generators

C. Insurance

D. Employee badges, guest sign-in, locks on computer room doors

E. Hot site

F. Intrusion detection systems

G. Off-site storage of backup computer programs and data

H. Training (personnel development)

I. Personnel termination procedures

J. Security guards

K. Program change controls

L. Operations run manuals

The following is a list of 10 situations that have control implications.

Situations

1. A computer programmer at Velux Company was fired for gross incompetence. During the two-week notice period, the programmer destroyed the documentation for all programs that he had developed since being hired.
2. A fire destroyed part of the computer room and the adjacent library of computer disks at Oak, Inc. It took several months to reconstruct the data from manual source documents and other hard copy records.
3. A competitor flooded the Lanesboro Company Web server with false messages (i.e., a denial-of-service attack). The Web server, unable to handle all of this traffic, shut down for several hours until the messages could be cleared.
4. A computer hacker created a program to generate random user IDs and passwords. He used the random number program to crack the computer system of Ajax, Inc.
5. A computer operator experienced an abnormal ending during the nightly run of updates to the inventory master data. In a state of panic, he woke his supervisor from a sound sleep at 3:00 A.M. to get help in getting the job restarted.
6. During the nightly computer run to update bank customers' accounts for deposits and withdrawals for that day, an electrical storm caused a temporary power failure. The run had to be reprocessed from the beginning, resulting in certain other computer jobs not being completed on schedule.
7. A group of demonstrators broke into a computer center and destroyed computer equipment worth several thousand dollars.
8. The computer users at the Darien Company do not know how to use the computer very well.

9. A disgruntled programmer at the Tracey Company planted a logic bomb in the computer program that produced weekly payroll checks. The bomb was triggered to go off if the programmer were ever terminated. When the programmer was fired for continued absenteeism, the next weekly payroll run destroyed all the company's payroll master data.

10. The computer systems at Coughlin, Inc. were destroyed in a recent fire. It took Coughlin several days to get its IT functions operating again.

Match the 10 situations with a control plan that would *best* prevent the system failure from occurring. Because there are 12 control plans, you should have 2 letters left over.

P 8-5 Assume that accounts payable are processed on a computer and that the options in the accounts payable system module are as follows:

1. Maintain vendor master data (i.e., add, change, or delete vendors in the vendor master data).
2. Record vendor invoices.
3. Record vendor credit memos.
4. Select vendor invoices for payment.
5. Print checks
6. Record payments.
7. Print accounts payable reports.

Further assume that personnel in the accounts payable department include the department manager and two clerks, R. Romeo and J. Juliet.

By placing a ''Y'' for yes or an ''N'' for no in the following table, show which users, if any, should (or should not) have access to each of the seven accounts payable options. Make and state whatever assumptions you think are necessary. In one or two paragraphs, explain how your matrix design would optimize the segregation of duties control plan.

Option	Manager	Romeo	Juliet
1	_____	_____	_____
2	_____	_____	_____
3	_____	_____	_____
4	_____	_____	_____
5	_____	_____	_____
6	_____	_____	_____
7	_____	_____	_____

P 8-6 Personnel at Saranac Company must perform the following functions:

1. Receive checks and remittance advice from customers.
2. Approve vendor invoices for payment and prepare checks.

3. Approve credit memoranda for customer sales returns.
4. Record collections on account from customers.
5. Record customer sales returns.
6. Make daily deposits of cash receipts.
7. Sign payment checks and mail them to vendors.
8. Record cash payments to vendors.
9. Record purchase returns and allowances.
10. Reconcile the bank account each month.

Saranac has 3 employees, Peter, Paul, and Mary, any of whom is capable of performing any of the 10 functions.

Explain how you would divide the 10 functions among the 3 employees to optimize the segregation of duties control plan discussed in the chapter. Consider only control aspects when allocating the duties. In other words, ignore factors such as the workload of each employee, except that any one employee should be assigned a minimum of 2 functions. Your solution should also include a one-paragraph explanation of how your design accomplishes the control goals that segregation of duties is supposed to achieve.

P 8-7 Research the Internet, newspapers, magazines, and journals to find recent incidences of outages of one or more Web sites. Develop a report (format and length to be determined by your instructor) describing how long the site(s) were not available and how it was they came to be out of service. Describe in your report which controls would have *prevented, detected,* or *corrected* the outages.

P 8-8 Research the Internet, newspapers, magazines, and journals to find recent incidences of *denial-of-service attacks* on one or more Web sites. Develop a report (format and length to be determined by your instructor) describing how long the site(s) were not available and how it was they came to be out of service. Describe in your report the controls which would have *prevented, detected,* or *corrected* the attacks and resulting outages.

P 8-9 The American Institute of Certified Public Accountants (AICPA) has adopted a framework called Trust Service Principles.

a. Look up this framework on the Internet and explain each of the principles.

b. What types of assurance services are already based on the Trust Service Principles?

c. Create two additional assurance services, not already in place or under consideration by the AICPA, which can use Trust Services Principles. For each additional service you recommend, explain which principles would apply, how, and why.

P 8-10 The following is a list of 12 control categories and specific control plans from this chapter.

Control Plans

A. Plan and Organize Domain

B. Segregation of duties

C. Systems Development Life Cycle (SDLC)

D. Security module

E. Business interruption planning

F. Application documentation

G. Monitor and Evaluate Domain

H. Control environment

I. Selection and hiring controls

J. Program change controls

K. Deliver and Support Domain

L. IT governance

The following is a list of 10 company-level controls from PCAOB Auditing Standard Number 2 (see AS2 paragraphs 50–53).

Company Level Controls

1. Tone at the top
2. Assignment of authority and responsibility
3. Consistent policies and procedures
4. Company-wide programs such as codes of conduct
5. Management's risk assessment process
6. Process to assess controls and results of operations
7. Controls over program development
8. Controls over program changes
9. Controls over computer operations
10. Controls over access to programs and data

Match the 10 company-level controls with a control category or control plan that would *best* exemplify the company-level control. Because there are 12 control categories and control plans, you should have 2 letters left over.

P 8-11 The following is a list of 10 common security problems. For each problem, describe why it is a problem and choose a control plan from this chapter that would prevent or detect the problem from occurring.

A. To keep track of the passwords used to access various computer systems, employees create Word documents listing their passwords and store the document with the name ''passwords.doc.''

B. Private and sensitive information is sent to multiple persons via e-mail. The e-mails include all addressee names within the e-mail address list.

C. An individual made millions by purchasing bank account information from eight employees of various banks. He had approximately 676,000 accounts in his database. Some bank employees were accessing up to 500 customer accounts each week to obtain the account information that they were selling.

D. Criminals posing as small business owners obtained names, addresses, and social security numbers from an organization whose business is to give such information only to legitimate customers who have a right to the data.

E. A financial analyst's laptop was stolen from his car. The laptop contained the names and social security numbers of 16,500 current and former employees.

F. Tapes that included information on 3.9 million credit card customers were lost in transit to a credit bureau. Data included names, social security numbers, account numbers, and payment histories.

G. An individual sold his PDA on eBay. The PDA contained hundreds of confidential e-mails.

H. An organization's top salesman uses a consumer grade instant messaging (IM) client (e.g., AOL Instant Messaging). Such clients bypass antivirus and spam software, don't have auditing and logging capabilities, and allow users to choose their IM name.

I. An executive of a financial services firm implements a wireless network so that she can work at home from anywhere in her house. After setting up the network she logs on using the default password.

J. A third-party processor of credit card transactions allowed an unauthorized individual to infiltrate its network and access cardholder data.