At 8:46 A.M. on September 11, 2001, American Airlines Flight 11 crashed into the north tower of the World Trade Center (WTC) in New York City. A short time later, at 9:02 A.M., United Airlines Flight 175 crashed into the south tower of the World Trade Center. Two other flights were hijacked that day and crashed; American Airlines Flight 77 crashed into the Pentagon near Washington, DC, and United Airlines Flight 93 exploded in a field 80 miles southeast of Pittsburgh. By the end of the next day it was believed that over 6,000 lives had been lost (this number started at over 10,000 and was later revised to less than 3,000) and several buildings in or near the sixteen-acre WTC complex had collapsed or had been severally damaged. Those buildings included: WTC buildings One and Two (the north and south towers), WTC buildings Three through Six, 3 World Financial Center, The Millennium Hotel, and 1 Liberty Plaza. Incredible human suffering, as well as numerous acts of kindness and bravery, resulted from this tragedy. The day-to-day lives of individuals, governments, and businesses were also affected in many predictable and some unforeseen ways.

In the aftermath of this tragedy airlines did not fly for several days, Wall Street trading was suspended for the remainder of the week, and hundreds of businesses located in and around the WTC struggled to resume anything that might resemble normal operations. To do so, these businesses needed to replace infrastructure such as offices, phones, computers, and data. At the same time, they needed to locate their personnel and put them back to work using new facilities. Companies and individuals throughout the world were also affected. For example, supply chains that depended on the airlines were disrupted, as were organizations with operations, communications, or technology infrastructures that had been in or around the WTC. These recovery activities tested, under the most extreme circumstances, organizations’ business continuity and contingency plans.

At almost the same time, events were unfolding in the fall of 2001 at Enron Corporation in Houston, Texas. These events, while not resulting in the same loss of lives and physical destruction as the events of September 11, would affect the lives of thousands and would have ramifications that would ripple throughout the world economy. Enron started the year 2001 as the seventh largest (in revenues) U.S. corporation, with a market value of $80 billion. During the course of the fall of 2001 it became known that Enron had overstated profits by $600 million over the previous four years. In November Enron issued revised financial statements to reflect correct numbers.
cember 2, 2001, Enron declared bankruptcy, the largest U.S. bankruptcy claim in history.

Enron stockholders lost $80 billion in investments. Employees and retirees, whose 401(k) plans contained Enron stock, experienced disproportionate losses. Enron management, while encouraging the general public and Enron employees to purchase Enron stock, had divested themselves of hundreds of millions of dollars of the soon-to-be worthless stock. To inflate its earnings, Enron had engaged in business transactions with partnerships controlled by its own officers and had concealed the true nature of these partnerships.

In January of 2002 we learned more about the scope of this legal and ethical scandal. After the problems at Enron surfaced, documents were shredded at Enron and at the offices of Enron’s auditors, Arthur Andersen. Enron V-P Sherron Watkins revealed a memo that she had sent to Enron CEO Kenneth Lay warning that accounting scandals might cause the downfall of Enron. As a result Enron became the target of Justice Department criminal probes, congressional and SEC investigations, and shareholder lawsuits.

**Synopsis**

Could a system of corporate governance, including internal control, have prevented the tragedies of September 11? Controls that might have prevented the hijackings and crashes are beyond the scope of this text. But, there are controls that would have prevented some of the resulting business losses. In many cases, existing controls, especially contingency plans, did assist in minimizing the impact on companies located at the WTC. There are also controls that could have prevented the accounting scandals at Enron. This chapter and Chapter 9 emphasize the importance of effectively controlling business processes to prevent such events or to minimize the losses that result from them. These chapters provide a solid foundation for later study of controls for specific business processes covered in Chapters 10 through 14.

Let’s consider how this chapter addresses our three themes. First, consider how important controls are to organizations that are tightly integrated internally—such as with enterprise systems—or have multiple connections to its environment—such as when they conduct e-business. Management must be confident that each component of the organization performs as expected and interacts well with related components or chaos will prevail. Second, organizations engaged in e-business must have control processes in place to reduce the possibilities of fraud and other disruptive events and to ensure compliance with applicable laws and regulations. For example, when engaged in Internet-based commerce, an organization may need to comply with relevant privacy regulations. Or, they may need to replace the infrastructure—Web sites, communications, and so on—in the event of tragedy. Finally, recognize that the success of most organizations today is partly determined by their ability to employ their technology resources effectively. In the second half of this chapter we discuss the control process—the management practices—that can ensure that an organization’s technology resources are directed at achieving the organization’s objectives, and that those resources remain available after events such as those on September 11.
LEARNING OBJECTIVES

- To explain why business organizations need to achieve an adequate level of internal control
- To explain the importance of internal control to organizational and IT governance, and business ethics
- To enumerate IT resources and explain how difficult it is to control them
- To describe management fraud, computer fraud, and computer abuse
- To describe the major IT control processes organizations use to manage their IT resources
- To identify operations and information process control goals and categories of control plans

Why Do We Need Control?

This chapter explores the strategies used to control the processes of a business organization. Recall from Chapter 1 that business organizations are composed of three major components: the management process, the operations process, and the information process. This chapter concentrates on controlling the entire business process (i.e., the combined management, operations, and information processes).

It is management’s responsibility to exercise control over the business process. The major reasons for exercising this control are (1) to provide reasonable assurance that the goals of each process are being achieved, (2) to mitigate the risk that the enterprise will be exposed to some type of harm, danger, or loss (including loss caused by fraud, natural disasters, and terrorist attacks, or other intentional and unintentional acts), and (3) to provide reasonable assurance that certain legal obligations, such as accurate financial reporting, are being met. The sections that follow address all of these reasons.

Corporate Governance

Picture yourself as the manager of customer sales and service at one of the insurance companies located in the World Trade Center. It is the afternoon of September 11. You are OK and have made your way across the Hudson River to New Jersey. Let’s say that you have been able to contact your family and friends and they are all OK. Now you want to reestablish customer services for your company; to provide customers with information about their coverage and to process claims. To do so you need an office, phones, computers, internal and external data networks, customer data, and customer service personnel.

Without the control processes that ordinarily exist, could you accomplish your objective of providing timely customer service? Perhaps; perhaps not. While we can argue that process objectives might be achieved in the absence of control, the primary reason for control is to help ensure that process goals are achieved. For example, you might be able to buy the infrastructure necessary to resume operations. But, unless you had a business continuity plan in place, you might not be able to locate key customer service personnel and restore your customer data. Thus, you may have a low probability of resuming operations in a timely manner.
Now assume that you are an employee (probably a former employee) at Enron. You were well paid and your retirement was secured with Enron stock. Now, after the bankruptcy declaration and resulting layoffs, you have no job and no financial assets. How did this happen? How could it have been prevented? Why didn’t Sherron Watkins’ memo result in changes to the accounting practices at Enron? Did Enron management really believe that these accounting practices would accomplish long- and short-run Enron objectives? Why did Andersen employees shred documents? Again, internal control can provide the mechanisms to develop and achieve objectives.

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission (National Commission on Fraudulent Financial Reporting) published a highly cited framework for internal control to help companies design effective control strategies. It says that "to effect control, there need to be predetermined objectives. Without objectives, control has no meaning (emphasis added)." The COSO report also states that control “involves influencing someone and/or something—such as an entity’s personnel, a business unit or an entire enterprise—with the purpose of moving toward the objectives.”1 In support of this point, a survey of 300 executives working for major companies based in the United States reported that executives who believed that their companies had strong internal control systems also believed that their companies were more likely to be successful in achieving corporate objectives, that their company’s return on equity had increased over the past three years, and that their company had been more profitable than its competitors.2

Rather than express the purpose of control in terms of the good to be achieved, we can also state its purpose in terms of the bad to be avoided. For instance, in our WTC illustration, is there a risk of not being able to resume operations in the long run? Yes! Therefore, a second reason for controlling systems is to lessen the risk that unwanted outcomes will occur. We define risk as the possibility that an event or action will cause an organization to fail to meet its objectives (or goals). Organizations must identify and assess the risk that untoward events or actions will occur and then reduce the possibility that those events or actions will occur by designing and implementing systems of control.

Internal control has recently become more important because of the emphasis placed by shareholders on corporate governance, demands placed on boards of directors and executives to implement and demonstrate control over business processes. The events at Enron, and later WorldCom and others, will make this even more important. Enterprise systems help provide this control, because they can support global, comprehensive, and integrated information sharing. In a recent example, Boston Scientific uncovered fraudulent sales records in its Japan office soon after SAP, an enterprise system, was installed. The ability to track sales globally triggered a closer look at unusual sales return patterns in the Japanese operations. At least one high-ranking corporate officer resigned as a result of this $70 million loss.

Executives, in turn, must implement and demonstrate governance of IT operations. Indeed, technology often represents a major portion of an organization’s costs. On the other hand, without that technology an organization could not perform important operational processes, make decisions, or survive. In both cases—corporate

---

and IT governance—frameworks for control, such as those introduced here and expanded upon throughout this text, will be key elements in this governance process. The events of September 11 forced all organizations to look more carefully at the strategies they had in place to recover from terrorist attacks and other such events. The Enron debacle will drive additional changes in the controls over the financial reporting process.

Let’s now examine a few of the added challenges that management must address when the organization is engaged in e-business. Organizations engaged in e-business must protect the privacy of any information that they may gather from their customers. They must install controls to provide assurance that their privacy-related practices comply with state and federal laws. Also, customers may choose to not do business with merchants that do not protect customer data consistent with their stated policies. The importance of privacy is illustrated by the rise of the Chief Privacy Officer, who is featured in Technology Excerpt 8.1.

Technology Excerpt 8.1

Chief Privacy Officers

Ronald Hoffman, the privacy issues manager at Mutual of Omaha Insurance Co., is in the forefront of a new breed of executives who are working with CIOs to set corporate data-privacy policies. Hoffman is responsible for helping to establish privacy practices for Mutual of Omaha. His job has become a key part of the Omaha-based insurer’s overall corporate strategy in response to new privacy regulations and an ongoing debate over whether the government should set more rules or allow companies to self-regulate themselves.

For Mutual of Omaha, it’s a bottom-line issue. Creating data-privacy policies and then standing behind them is “something that is going to help build a trusting relationship with our customers that we hope will allow us to retain their business and acquire new business,” said Hoffman.

Hoffman is currently working with Mutual of Omaha’s information technology managers to document the way data flows through all of the company’s systems in order to learn exactly what happens to the information and who has access to it.

“We really didn’t have a good handle on information flows through the company,” Hoffman said. But the documentation project now under way should lead to better risk management and security assessments in addition to helping the insurer develop its privacy policies, he added.

Corporate privacy officers work with a variety of corporate departments, including information systems, legal affairs, governmental affairs, and employee training. But the most important thing they need is buy-in from top management, said Tatiana Gau, vice president of integrity assurance at America Online Inc.

“There’s no question in my mind that one of the most important roles of the Chief Privacy Officer (CPO) is to ensure that the whole company is adhering to a privacy commitment,” Gau said. At AOL, for example, the importance of data privacy has been “baked into all the lifecycles” of the company, she added.

Fraud and Its Relationship to Control

Was the scandal at Enron the result of fraud, or poor—perhaps unethical—management practices? In this section, we discuss management fraud, computer fraud, and computer abuse. Let’s begin by defining fraud as a deliberate act or untruth intended to obtain unfair or unlawful gain. Management’s legal responsibility to prevent fraud and other irregularities is implied by laws such as the Foreign Corrupt Practices Act,3 which states “a fundamental aspect of management’s stewardship responsibility is to provide shareholders with reasonable assurance that the business is adequately controlled.” Instances of fraud undermine management’s ability to convince the various authorities that it is upholding its stewardship responsibility.

Why are Congress, the financial community, and others so impassioned about the subject of fraud? In some highly publicized business failures that caught people completely by surprise, financial statements showed businesses that were prospering. Tinkering with the financial statements, as at Enron, causes hardship or failure for many firms and individuals.

Let’s examine some fraud-related problems that management must address when the organization is engaged in e-business. First, an organization that receives payment via credit card, where the credit card is not present during the transaction (e.g., sales via telephone or Web site), absorbs the loss if a transaction is fraudulent. To prevent this, the organization may install controls, such as antifraud software. Some banks will drop merchants who have unacceptably high fraud rates.

The proliferation of computers in business organizations has created expanded opportunities for criminal infiltration. Computers have been used to commit a wide variety of crimes, including fraud, larceny, and embezzlement. In general, these types of computer-related crimes have been referred to as computer fraud, computer abuse, or computer crime. Technology Insight 8.1 (page 246) describes some of the better-known techniques used to commit computer fraud or to damage computer resources.

Be aware of two things: insiders commit the majority of computer crimes, and the methods listed in the summary are by no means exhaustive. For instance, two abuses not shown in Technology Insight 8.1 that typically are perpetrated by someone outside the organization are computer hacking and computer viruses. Technology Insight 8.2 (page 247) has a brief explanation of computer viruses. Both of these computer crimes, spreading viruses and hacking, are a major concern to organizations engaged in e-business because they affect the actual and perceived reliability and integrity of their electronic infrastructure.

Here are three important facts to remember. First, those who have authorized access to the targeted computer perpetrate the majority of malicious acts. Second, it has been estimated that losses due to accidental, nonmalicious acts far exceed those caused by willful, intentional misdeeds. Third, the manipulation of events (i.e., adding, changing, or deleting of events) is one frequently employed method of committing computer fraud. The most cost-effective method for minimizing simple, innocent errors and omissions as well as acts of intentional computer crimes and fraud is to apply normal controls within existing systems conscientiously.

Computer Abuse Technologies

Salami. Unauthorized instructions are inserted into a program to steal very small amounts. For example, a program is written to calculate daily interest on savings accounts. A dishonest programmer includes an instruction that if the amount of interest to be credited to the account is other than an even penny (for example, $2.7345)—the excess over the even amount (.0045) is to be credited to the programmer’s account. While each credit to his account is minute, the total can accumulate very rapidly.

Trap Door (back door). During the development of a program, the programmer may insert a special code or password that enables him to bypass the security features of the program in order to simplify his work. These features are meant to be removed when the programmer’s work is done, but sometimes they aren’t. Someone who knows the code or password can still get into the program.

Logic Bomb. Similar to the trap door, unauthorized code is inserted into a program at a time when a programmer has legitimate access to the program. When activated, the code causes a disaster, such as shutting the system down or destroying data. The technique is usually tied to a specific future date or event, in which case it is a time bomb. For example, if the programmer’s name no longer appears on the payroll records of the company, the bomb is activated and the disaster occurs.

Trojan Horse. Like a Logic Bomb, a Trojan Horse is a module of unauthorized instructions covertly placed in a program; a Trojan Horse, unlike the Logic Bomb, lets the program execute its intended function while also performing an unauthorized act. Some Trojan Horses are distributed by e-mail to steal passwords. This was an element of the ILOVEYOU virus of May 2000.

Worm. A program that replicates itself on disks, in memory, and across networks. It uses computing resources to the point of denying access to these resources to others, thus effectively shutting down the system. They also may delete files and be spread via e-mail. Many recent viruses have included these worm features.

Zombie. A program that secretly takes over another Internet-attached computer, then uses that computer to launch attacks that can’t be traced to the zombie’s creator. Zombies are elements of the denial-of-service attacks discussed in this chapter.

A **computer virus** is a program that can attach itself to other programs (including macros within word processing documents), thereby “infecting” those programs and macros. Computer viruses may also be inserted into the boot sectors* of PCs. Viruses are activated when you run an infected program, open an infected document, or boot the computer from an infected disk. Computer viruses alter their “host” programs, destroy data, or render computer resources (e.g., disk drives, central processor, networks) unavailable for use. Unlike other malicious programs such as logic bombs and Trojan Horses, viruses differ in that they reproduce themselves in other programs.

Some viruses are fairly innocent—they might merely produce a message such as “GOTCHA” or play “The Blue Danube” through the computer’s speakers. Other viruses can be more harmful. Some viruses delete programs and files; some even reformat the hard drive, thus wiping away all that is stored there. Finally, there are some viruses that will overload your network with “messages,” making it impossible to send or receive e-mail or to connect to external sources, such as the Internet.

Many viruses first enter an organization through PCs; many have been introduced via electronic bulletin boards, shared software, and files attached to e-mail messages. This sharing allows viruses to become an epidemic like a biological virus. The real fear that causes information systems managers to lose sleep, of course, is that the virus will spread to the organization’s networks (and networked computing resources) and destroy the organization’s most sensitive data.

In May 2000, the “ILOVEYOU” virus quickly spread throughout the world, infecting a million computers. This virus was written in Visual Basic script (file extension .vbs) and came attached to an e-mail message. If the recipient launched the program, the virus deleted artwork files and altered music files. If the victim was using the Microsoft Outlook mail program, the virus mailed itself to everyone in the victim’s e-mail address book. Thus, the “ILOVEYOU” virus would set a trap for many others who would think they were getting mail from a colleague. Finally, the virus contained a Trojan Horse that mailed victim passwords to an e-mail account in the Philippines.

How does one protect from a viral infection? If you are going to share files and disks with others, use virus protection software to scan all files and disks before the disks are used or the files are opened. This is, of course, especially true of files received as e-mail attachments. Don’t open e-mail from people you don’t know. Don’t open e-mail with .xxx or .xbs extensions. Back up files regularly. Use an up-to-date anti-virus program to scan your hard disk regularly. E-mail servers could be set to block attachments written in Visual Basic script.

---

*The boot sector is the area of a hard or floppy disk containing the program that loads the operating system.

Defining Internal Control

In the preceding sections, we discussed the importance of an organization achieving an adequate level of internal control. But what do we mean by internal control? The COSO report mentioned earlier in the chapter emphasizes that internal control is a process. A process is a series of actions or operations leading to a particular and usually desirable result. Results could be effective internal control, or a specified output for a particular market or customer. The idea of process is important to our understanding of internal control and business processes in modern organizations. Armed with this perspective, let’s proceed to a working definition of internal control to use throughout the text.

A Working Definition of Internal Control

Internal control is a system of integrated elements—people, structure, processes, and procedures—acting together to provide reasonable assurance that an organization achieves its business process goals. The design and operation of the internal control system is the responsibility of top management and therefore should:

◊ Reflect management’s careful assessment of risks.
◊ Be based on management’s evaluation of costs versus benefits.
◊ Be built on management’s strong sense of business ethics and personal integrity.

Before discussing two key elements of the definition, which we call control goals and control plans, let’s pause to examine the underpinnings of the system—namely, its ethical foundation. As you read this section, consider the events that unfolded at Enron.

Ethical Considerations and the Control Environment

COSO places integrity and ethical values at the heart of what it calls the control environment. In arguing the importance of integrity and ethics, COSO makes the case that the best designed control systems are subject to failure caused by human error,

---

4 The COSO definition of internal control has become widely accepted and the basis for definitions of control adopted for other international control frameworks: Internal control is a process—affected by an entity’s board of directors, management, and other personnel—designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

• Effectiveness and efficiency of operations
• Reliability of financial reporting
• Compliance with applicable laws and regulations

Internal Control—Integrated Framework—Framework Volume (New York, NY: The Committee of Sponsoring Organizations of the Treadway Commission, 1992): 9, 12 and 14. Our working definition of control, presented in the next section, classifies control goals into two broad groups only—those for the operations process and those for the information process. Our two groupings roughly parallel the first two COSO categories. In our control framework and control matrices in this and later chapters, we include COSO’s third category—compliance with applicable laws, regulations, and contractual agreements—as one of the control goals of the operations processes.
faulty judgment, circumvention through collusion, and management override of the system. COSO goes on to state that:

Ethical behavior and management integrity are a product of the “corporate culture.” Corporate culture includes ethical and behavioral standards, how they are communicated and how they are reinforced in practice. Official policies specify what management wants to happen. Corporate culture determines what actually happens, and which rules are obeyed, bent or ignored.\textsuperscript{5}

Management is responsible for internal control and can respond to this requirement legally or by creating a “control environment.” That is, management can follow the “letter of the law” (its form), or it can respond \textit{substantively} to the need for control. The \textit{control environment} reflects the organization’s (primarily the board of directors’ and management’s) general awareness of and commitment to the importance of control throughout the organization. In other words, by setting the example and by addressing the need for control at the top of the organization, management can make an organization \textit{control conscious}.

For example, reward systems might consider ethical, legal, and social performance, as well as the bottom line. Strategies should be developed so as not to create conflicts between business performance and legal requirements. Management should consistently find it unacceptable for personnel to circumvent the organization’s system of controls and, as importantly, \textit{should impose stiff sanctions for such unacceptable behavior}. These actions are included in what some call the “tone at the top” of the organization. Some question whether the large campaign contributions made by Enron and its executives set the proper tone at the top of that organization.

A number of companies have articulated the ethical behavior expected of employees in a very tangible way by developing corporate \textit{codes of conduct} that are periodically acknowledged (i.e., signed) by employees. The codes often address such matters as illegal or improper payments, conflicts of interest, insider trading, computer ethics, and software piracy.

\section*{Business Process Control Goals and Control Plans}

Our working definition of \textit{internal control} describes it in the broad sense of both selecting the ends to be attained (\textit{control goals}) and specifying the means to ensure that the goals are attained (\textit{control plans}). Control also extends to the processes of reviewing a system periodically to ensure that the goals of the system are being achieved, and to taking remedial action (if necessary) to correct any deficiencies in the system (i.e., monitoring). Control is concerned with discovering courses of action that contribute to the general welfare of the business organization and with ensuring that the implementation of these actions produces the desired effects.

\textit{Control goals} are business process objectives that an internal control system is designed to achieve. Table 8.1 (page 250) provides an overview of the \textit{generic} control goals of the \textit{operations process} and of the \textit{information process}. To illustrate our discussion we use a cash receipts process, similar to the Causeway system depicted in Figure 2.13 (page 54).

### Table 8.1  Control Goals

<table>
<thead>
<tr>
<th>Control goal</th>
<th>Definitions</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control goals of the operations process</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure <strong>effectiveness</strong> of operations by achieving the following operations process goals: (itemize the specific goals for the process being analyzed)</td>
<td><strong>Effectiveness:</strong> A measure of success in meeting one or more goals</td>
<td>Did we achieve our goal? If my goal was to get an A in the course, did I get an A?</td>
</tr>
<tr>
<td>Ensure <strong>efficient</strong> employment of resources</td>
<td><strong>Operations process goals:</strong> Criteria used to judge the effectiveness of an operations process</td>
<td>If our goal is to deposit cash receipts on the day received, we are effective if cash receipts are deposited on the day received.</td>
</tr>
<tr>
<td>Ensure <strong>security</strong> of resources. (specify the applicable operations process and information process resources)</td>
<td><strong>Security of resources:</strong> Protecting an organization’s resources from loss, destruction, disclosure, copying, sale, or other misuse</td>
<td>Are the physical (e.g., cash) and nonphysical (e.g., information) resources available when required? Are they put to unauthorized use?</td>
</tr>
<tr>
<td><strong>Control goals of the information process</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure <strong>input validity</strong> (IV)</td>
<td><strong>Input validity:</strong> A control goal that requires that input data be appropriately approved and represent actual economic events and objects</td>
<td>Are all of the cash receipts to be input into our computer supported by actual customer payments?</td>
</tr>
<tr>
<td>Ensure <strong>input completeness</strong> (IC)</td>
<td><strong>Input completeness:</strong> A control goal that requires that every valid event or object be captured and entered into a system</td>
<td>Are all valid customer payments captured on a remittance advice (RA) and entered into our computer?</td>
</tr>
<tr>
<td>Ensure <strong>input accuracy</strong> (IA)</td>
<td><strong>Input accuracy:</strong> A control goal that requires that events be correctly captured and entered into a system</td>
<td>Is the correct payment amount and customer number transcribed onto the RA? Is the correct payment amount and customer number keyed into our computer? Is the customer number missing from the RA?</td>
</tr>
<tr>
<td>Ensure <strong>update completeness</strong></td>
<td><strong>Update completeness:</strong> A control goal that requires that all events entered into a computer are reflected in their respective master data</td>
<td>Have all input cash receipts been recorded in our accounts receivable master data?</td>
</tr>
<tr>
<td>Ensure <strong>update accuracy</strong></td>
<td><strong>Update accuracy:</strong> A control goal that requires that data entered into a computer are reflected correctly in their respective master data</td>
<td>Are all input cash receipts correctly recorded in our accounts receivable master data?</td>
</tr>
</tbody>
</table>
Control Goals of the Operations Process

The first control goal, ensure effectiveness of operations, strives to ensure that a given operations process (e.g., our cash receipts process) is fulfilling the purpose for which it was intended. Notice that we must itemize the specific operations process goals. These goals are specific to each organization and no uniform set of operations goals exists. In each of the business process chapters, we provide a representative listing of operations process goals. The next goal, ensure efficient employment of resources, can be evaluated in only a relative sense. For example, let’s assume that one goal is to deposit all cash on the day received. To determine efficiency we would need to know the cost of the people and computer equipment required to accomplish this goal. If the cost is more than the benefits obtained (e.g., security of the cash, interest earned), the system might be considered inefficient. Likewise, if our system costs more to operate than a system in a similar organization, we would judge the system to be inefficient.

Let’s now discuss the last operations process control goal in Table 8.1, to ensure security of resources. As noted in the table, resources take many forms, both physical and nonphysical. Information has become a key resource of most organizations. For example, the information about our customers (as stored in the accounts receivable master data) is very valuable for this company. An organization must protect all of its resources, both tangible and intangible.

Control Goals of the Information Process

A glance at Table 8.1 reveals that the first three control goals of the information process deal with entering event-related data into a system. Recall from Chapter 1 that data input includes capturing data (for example, completing a source document such as a sales order, or, in the case of a cash receipts system, writing the check number and amount on the RA). Data input also includes, if necessary, converting the data to machine-readable form (for example, keying in the remittance advices to add events to the cash receipts events data). Therefore, events data are the subjects of the input control goals shown in Table 8.1.

These three control goals trigger the following questions: “Did the event occur?” (input validity); “Is there a record of each event?” (input completeness); and “Is the record correct?” (input accuracy). Thinking about these control categories in this way may help you to identify controls that provide adequate coverage across all the categories.

To illustrate the importance of achieving the first goal, ensure input validity, assume that our accounts receivable clerk processes a batch of 50 cash receipts (including their payment stubs, or RAs). Further assume that two of the 50 RAs represent fictitious cash receipts (for example, a mailroom employee fabricates phony remittance advices for relatives who are customers). What is the effect of processing the 50 RAs including the 2 fictitious remittances? First, the cash receipts event data and the accounts receivable master data each have been corrupted by the addition of two fictitious cash receipts.

As mentioned earlier in the chapter, we also include compliance with applicable laws, regulations, and contractual agreements (i.e., COSO’s third category of entity objectives) as one of the goals of each operations process to which such laws, regulations, or agreements might be appropriate. For instance, compliance with the Robinson/Patman Act is shown as a legitimate goal of the order entry/sales process in Chapter 10.
bogus RAs. Second, if not detected and corrected, the pollution of these data will result in unreliable financial statements—overstated cash and understated accounts receivable—and other erroneous system outputs (e.g., cash receipts listings, customer monthly statements).

To discuss the second information process goal, *ensure input completeness*, let’s return to the previous example and suppose that, while the 48 valid RAs are being key entered (we’ll ignore the two fictitious receipts in this example), the accounts receivable clerk decides to get a cup of coffee. As the clerk walks past the batch of 48 RAs, 10 are blown to the floor and are not entered into the system. What is the effect of processing 38 RAs, rather than the original 48? First, the cash receipts transaction data will be incomplete; that is, it will fail to reflect the true number of remittance events. Second, the incompleteness of the data will cause the resulting financial statements and other reports to be unreliable (i.e., understated cash balance and overstated accounts receivable). In this example, the omission was unintentional. Likewise, fraudulent, intentional misstatements of organizational data can be accomplished by omitting some events.

When dealing with input completeness, we are concerned with the existence of documents or records representing an event or object, not the correctness or accuracy of the document or record. Accuracy issues are addressed by the third information process goal, *ensure input accuracy*. This goal relates to the various data fields that usually constitute a record of an event, such as a source document. To achieve this goal, we must minimize discrepancies between data items entered into a system and the economic events or objects they represent. Mathematical mistakes and the inaccurate transcription of data from one document or medium to another may cause accuracy errors. Again, let’s return to our example. Suppose that one of the valid RAs is from Acme Company, customer 159, in the amount of $125. The accounts receivable clerk mistakenly enters the customer number as 195, resulting in Ajax, Inc.’s account (rather than Acme’s) being credited with the $125.

Missing data fields on a source document or computer screen represent another type of accuracy error. For example, the absence of a customer number on a remittance advice would result in “unapplied” cash receipts (that is, receipts that can’t be credited to a particular customer). We consider this type of system malfunction to be an accuracy error rather than a completeness error, because the mere presence of the source document suggests that the event itself has been captured and that the input data are, by our definition, therefore complete.

Now let’s examine the last two information process control goals shown in Table 8.1. These goals deal with updating master data. As we learned in Chapter 1, master data update is an information processing activity whose function is to incorporate new data into existing master data. We also learned that there are two types of updates that can be made to master data: information processing and data maintenance. In this textbook, we emphasize information processing; therefore, our analysis of the internal controls related to data updates is restricted to data updates from information processing.

In our cash receipts system, the goal of update completeness relates to crediting customer balances in the accounts receivable master data for all cash collections recorded in the cash receipts event data. The goal of *ensure update accuracy* relates to correctly crediting (e.g., correct customer, correct amount) customer balances in the accounts receivable master data.

Once valid data have been completely and accurately entered into a computer (i.e., added to event data such as our cash receipts event data), the data usually go through
a series of processing steps. Several things can go wrong with the data once they have been entered into a computer for processing. Accordingly, the goals of update completeness and accuracy are aimed at minimizing processing errors. We should note, however, that if the events are processed using an online real-time processing system such as the one depicted in Figure 4.3 (page 114), the input and update will occur nearly simultaneously. This will minimize the possibility that the update will be incomplete or inaccurate.

**Control Plans**

Control plans are information processing policies and procedures that assist in accomplishing control goals. Control plans can be classified in a number of different ways that help us to understand them. Figure 8.1 (page 254) shows one such classification scheme—a control hierarchy that relates control plans to the control environment, defined earlier. The fact that the control environment appears at the top of the hierarchy illustrates that the control environment comprises a multitude of factors that can either reinforce or mitigate the effectiveness of the pervasive and process control plans.

The second level in the Figure 8.1 control hierarchy consists of pervasive control plans. Pervasive control plans relate to a multitude of goals and processes. Like the control environment, they provide a climate or set of surrounding conditions in which the various business processes operate. They are broad in scope and apply equally to all business processes—hence, they pervade all systems. For example, preventing unauthorized access to the computer system would protect all of the specific business processes that run on the computer (such as sales and marketing, billing, “purchase-to-pay,” business reporting, and so on). We discuss a major subset of these pervasive controls—IT processes (i.e., controls)—later in this chapter.

Process control plans are those controls particular to a specific process or sub-system, such as inventory or human resources, or to a particular mode of processing events, such as online or batch. Process control plans are the subject of the control framework introduced in Chapter 9.

Another useful and common way to classify controls is in relation to the timing of their occurrence. Preventive control plans stop problems from occurring. Detective control plans discover that problems have occurred. Corrective control plans rectify problems that have occurred. Let’s use the WTC tragedy to illustrate. By operating two computer processing sites—one primary and one mirror site—companies located in the WTC could prevent the loss of their computer processing capabilities and the data and programs stored on the computers located in the WTC (i.e., duplicate copies would reside at the mirror site). Smoke and fire detectors could detect fires in the building that inevitably lead to the loss of processing capabilities. Other monitoring devices could detect the loss of phones, data communications, and processing capabilities. These devices, operating at an organization’s facilities outside the WTC area, could have alerted company personnel to the loss of resources in the area of the WTC. Also, organizations can subscribe to services that will provide notification in the event of disaster. Finally, backup copies of programs and data could have been loaded onto computers at sites outside the WTC area to reinstate computer processing and related services. These are corrective controls because they replace data and services that were lost.
Introduction to Pervasive Controls

We begin our discussion of pervasive controls by introducing four broad IT control process domains and explain how IT control processes are directed at the control of IT resources and the attainment of the information qualities. Exhibit 8.1 defines IT resources that must be managed by the control processes. According to COBIT these IT resources must be managed to ensure that the organization has the information...
that it needs to achieve its objectives. COBIT also describes the qualities that this information must exhibit in order for it to be of value to the organization. These qualities are defined in Exhibit 1.1 (page 17).

We must determine how we can protect an organization’s computer from misuse, intentional or inadvertent, from within and from outside the organization. Pervasive controls are directed at answering the following questions. How can 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, will we be able to continue our operations? What policies and procedures can 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? An organization’s Information Systems function (ISF) is the department that develops and operates an organization’s Information System. The function (department) is composed of people, procedures, and equipment. This function is the object of many of the IT controls and its management, at the same time, is responsible for the implementation and operation of these processes.

## Four Broad IT Control Process Domains

COBIT groups IT control processes into four broad domains: (1) planning and organization, (2) acquisition and implementation, (3) delivery and support, and (4) monitoring. Figure 8.2 (page 256) depicts the relationship among these four domains and lists the IT control processes within each domain. Notice that the monitoring domain provides feedback to the other three domains. In the remainder of this chapter we discuss these ten IT control processes.

Before we move on to a discussion of the ten IT control processes, let’s discuss the concept of a control process. 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,

---

**Review Question**

Name and describe the five IT resources.

**Review Question**

What are the four IT control process domains?

---

**Exhibit 8.1** IT Resources

| Data: | Objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc. |
| Application systems: | Application systems are understood to be the sum of manual and programmed procedures. |
| Technology: | Technology covers hardware, operating systems, database management systems, networking, multimedia, etc. |
| Facilities: | Facilities are all resources to house and support information systems. |
| People: | People resources include staff skills, awareness, and productivity to plan, organize, acquire, deliver, support, and monitor information systems and services. |

which will bring about achievement of an organization’s objectives. It is through a coordinated effort, across all IT resources and all organizational units, that the objectives of the organization are achieved.

### Planning and Organization Domain

Within the planning and organization domain are processes to develop the strategy and tactics for an organization’s information technology. The overriding goal of these processes is to identify ways that IT can best contribute to the achievement of the organization’s objectives. Then, management must communicate that strategic vision to interested parties (within 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 requirements, 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 business requirements, management of the information systems 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 IT is used to the best advantage of the organization. An organization wants to be sure that the ISF is prepared to anticipate the competition’s actions and to take advantage of emerging IT. 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.

Elements of the strategic plan can help the organization achieve important enterprise systems, e-business, and technology objectives. For example, plans for any new lines of business, such as Internet ordering and payment, or changes in business processes, resulting from changes to an enterprise system, will require new data and new relationships among the data. These data elements and relationships must be incorporated into the organization’s information architecture model. The plan must also include processes to review IT capabilities to ensure that there is adequate technology to perform the IS function and to take advantage of emerging technology. Finally, the plan must contain procedures that ensure compliance with laws and regulations, especially those related to e-business (e.g., privacy, transborder data flows).

IT Process 2: Develop Tactics to Plan, Communicate, And Manage Realization of the Strategic Mission

To ensure adequate funding for IT, controlled disbursement of financial resources, and effective and efficient utilization of IT resources, IT resources must be managed through use of information services capital and operating budgets, by justifying IT expenditures, and by monitoring costs (in light of risks).

To ensure the overall effectiveness of the ISF, IS 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. IS management’s direction and policies must be consistent with the control environment established by the organization’s senior management.

To ensure that projects are completed on time and within budget and that projects are undertaken in order of importance, 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 organizational control plans for the information systems function.

**Segregation of duties control plan.** 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. Segregation of duties consists of separating the four basic functions of event processing. The functions are:

- **Function 1:** authorizing events.
- **Function 2:** executing events.
- **Function 3:** recording events.
- **Function 4:** safeguarding resources resulting from consummating events.

A brief scenario should illustrate this concept. 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 typical 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.

Now, 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, there would need to be collusion between one or more persons (departments) in order to exploit the system and conceal the abuse. Whenever collusion is necessary to commit a fraud, there is a greater likelihood that the perpetrators will be deterred by the risks associated with pursuing a colluding partner and that they will be caught.

Controls to prevent unauthorized execution of events ensure 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 machines 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 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 events within some predetermined credit limits. Digital signatures on electronic documents also authenticate or authorize requests from external parties, as seen in Technology Excerpt 8.2 (page 260). These procedures receive management authorization when the system is approved during initial development, or when the system is changed.

**Organizational control plans for the information systems function.** The information systems function normally acts in a service capacity for other operating units in the organization. In this capacity, it should be limited to carrying out function 3 of Table 8.2, recording events and posting event summaries. Approving and executing events along with safeguarding resources should be carried out by departments other than the ISF. This arrangement allows for effective implementation of segregation of duties. There are situations, however, where the functional divisions we mentioned can be violated. For instance, some ISFs do authorize and execute events; for example, the computer might be programmed to approve customer orders.

Within the ISF, we segregate duties to control unauthorized use of and/or changes to the computer and its stored data and programs. Segregation of duties within the ISF can be accomplished in a number of ways. One method of separating systems de-

---

**Table 8.2 Illustration of Segregation of Duties**

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Function 3</th>
<th>Function 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authorizing Events</strong></td>
<td><strong>Executing Events</strong></td>
<td><strong>Recording Events</strong></td>
<td><strong>Safeguarding Resources Resulting from Consummating Events</strong></td>
</tr>
<tr>
<td>Approve steps of event processing.</td>
<td>Physically move resources.</td>
<td>Record events in the appropriate data store(s).</td>
<td>Physically protect resources.</td>
</tr>
<tr>
<td>Approve picking inventory and sending inventory to shipping department.</td>
<td>Complete source documents.</td>
<td>Post event summaries to the master data store.</td>
<td>Maintain accountability of physical resources.</td>
</tr>
</tbody>
</table>

**Example: Processing a credit sales event.**

<table>
<thead>
<tr>
<th>Authorizing Events</th>
<th>Physical Movement of Resources</th>
<th>Record Event Details</th>
<th>Physically Protect Resources</th>
<th>Maintain Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve customer credit.</td>
<td>Pick inventory from bins.</td>
<td>Update accounts receivable, sales, and inventory event data.</td>
<td>Safeguard inventory while in storage at warehouse, while in transit to shipping department, and while preparing for shipment to customer.</td>
<td>Examine and count inventory periodically, and compare physical total to recorded total.</td>
</tr>
<tr>
<td>Approve picking inventory and sending inventory to shipping department.</td>
<td>Move inventory from warehouse to shipping department.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve shipping inventory to customer.</td>
<td>Ship inventory to customer.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve recording accounting entries.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Complete Source Documents**

- Enter sales order.
- Enter shipping document.
- Enter invoice.
Development and operations is to prevent programmers from operating the computer; thus reducing the possibilities of unauthorized data input or unauthorized modification of organizational data and programs. Passwords, assigned by an information security specialist, are critical to separating key functions between the ISF and operational units within the ISF.

Personnel Control Plans IT personnel resources must be managed to maximize their contributions to IT processes. 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 honest, competent employees will find it virtually impossible to implement other control plans.

The personnel control plans described in Table 8.3 help to protect an organization against certain types of risks. As you study each plan, think of the problems that
the plan can prevent or the control goal that could be achieved by implementing the plan. Also, consider how much more important these plans are when we consider the impact that they have on systems personnel.

Three plans in Table 8.3 require a little discussion. The control notion underlying rotation of duties and forced vacation is that if an employee is perpetrating some kind of irregularity, it will be detected by his/her 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., a preventive control). Beyond the control considerations involved, these two plans also help to mitigate the disruption that might be caused when an employee leaves the organization. When another person is familiar with the job duties of each position, no single employee is irreplaceable.

Finally, rigorous application of personnel termination policies is particularly important in the ISF. Disgruntled employees working in the ISF have the opportunity to cause much damage in a short time. For example, computer operations personnel could erase large databases in a matter of minutes. For this reason, key employees who have access to important programs and databases may be asked to leave the facility immediately, and in some cases, company security personnel may escort them from the premises.
Acquisition and Implementation

Within the acquisition and implementation domain are processes to identify, develop or acquire, implement IT solutions, and integrate them into the business processes. Once installed, procedures must also be in place to maintain and manage changes to existing systems. 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 update the wrong data or perform calculations incorrectly. Or, we may not complete the development on time and within budget. Finally, should we fail to develop proper controls for the new system, we could experience inventory shortages, inaccurate record keeping, or financial loss.

IT Process 3: Identify Automated Solutions

To ensure the selection of the best approach to satisfying users’ IT requirements, an organization’s Systems Development Life Cycle (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 information technology plan and the technology infrastructure and information architecture contained therein.

IT Process 4: Develop and Acquire IT Solutions

Once IT solutions have been identified and approval to proceed has been received, development—and/or appropriate acquisition—of the application software, infrastructure, and procedures may begin. 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. Design specifications include those for inputs, outputs, processes, programs, and databases.

The SDLC should also include procedures to ensure that platforms (hardware and systems software) support the new or modified application. Further, there should be an assessment 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 so as to continue to support existing or revised business processes.

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 are benchmarks for service on a Web site or to and from business partners engaged in electronic commerce.
IT Process 5: Integrate IT Solutions into Operational Processes

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. 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, highly integrated, business 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. Program change controls provide assurance that all modifications to programs are authorized, and ensure that the changes are completed, tested, and properly implemented. Changes in documentation should mirror the changes made to the related programs. Figure 8.3 (page 264) depicts the stages through which programs should progress to ensure that only authorized and tested programs are placed in production, which means that the programs are in use by the organization in the conduct of business. Notice that separate organizational entities 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 can be disastrous. For example, let’s say that a change is made to the inventory module of an enterprise system without testing to see the impact that change will have on the sales module used to enter customer orders. Since 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.

Delivery and Support

Within the delivery and support domain are processes to deliver required IT services, ensure security and continuity of services, set up support services, including training, and ensure integrity of application data. Failure of these processes can result in computing resources being lost or destroyed, becoming unavailable for use, or leading to unauthorized use of computing resources.

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 planning and organization domain, and developed
and implemented by the IT processes in the acquisition and implementation domain. Table 8.4 describes some of the key service-delivery activities.

**IT Process 8: Ensure Security and Continuous Service**

The IS 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 potential losses of usable resources. To ensure that sufficient IT resources remain available, management should establish a process to monitor the capacity and performance of all IT resources. For example, the actual activity on an organization’s Web site must be measured and additional capacity added as needed. 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, technology, and facilities, and to prevent use of unauthorized assets. To ensure that IT resources 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 below: 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, that includes disaster recovery/contingency 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 operations—for both the organization and its business partners. Catastrophic events, such as those experienced on September 11, 2001, have resulted in a heightened awareness of the importance of these controls. The types of backup and recovery covered in this section have been referred to in a variety of ways, including but not limited to: disaster recovery planning,
tingency planning, business interruption planning, and business continuity planning. Regardless of the label, these controls must include a heavy dose of pre-loss planning that will reasonably ensure post-loss recovery.

Before we go further, let us note that contingency planning extends much beyond the mere backup and recovery of stored computer data, programs, and documentation. The planning involves procedures for backing up the physical computer facilities, computer, and other equipment (such as communications equipment—a vital resource in the event of a catastrophe), supplies, and personnel. Furthermore, planning reaches beyond the IS function to provide backup for these same resources residing in operational business units of the organization. Finally, the plan may extend beyond the organization for key resources provided by third parties. You might also note that the current thinking is that we plan contingencies for important processes rather than individual resources. So, we develop a contingency plan for our Internet presence, rather than for our Web servers, networks, and other related resources that enable that presence.

Numerous disaster backup and recovery strategies may be included in an organization’s contingency plan. Some industries require instant recovery and must incur the cost of maintaining two or more sites. One such option is to run two processing sites, a primary and a mirror site that maintains copies of the primary site’s programs and data. During normal processing activities, master data is updated at both the primary and mirror sites. Located miles away from the primary site, the mirror site can take over in seconds if the primary site goes down. Mirror sites are very popular with airline and e-business organizations because they need to keep their systems and In-

<table>
<thead>
<tr>
<th>Table 8.4 Delivering Required Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity</strong></td>
</tr>
<tr>
<td>Define service levels</td>
</tr>
<tr>
<td>Manage third-party services</td>
</tr>
<tr>
<td>Manage IT operations</td>
</tr>
<tr>
<td>Manage data</td>
</tr>
<tr>
<td>Identify and allocate costs</td>
</tr>
</tbody>
</table>
ternet commerce sites online at all times. Server clustering can also be used to disperse processing load among servers so that if one server fails, another can take over.\(^8\) These clustered servers are essentially mirror sites for each other.

Here is one example of the importance of these contingency processes to e-business. In June 1999 the Web site for eBay, Inc., the online auctioneer, was unavailable for 22 hours. This downtime caused eBay to forego $3 to $5 million in fees and some erosion of customer loyalty. This failure spurred eBay to accelerate its plans for a better backup system.\(^9\)

For most companies, maintaining duplicate equipment is simply cost-prohibitive. Therefore, 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—sometimes up to 100 companies—and that is made available to client companies for a monthly subscriber’s fee. Less costly, but obviously less responsive, is a cold site. It is a facility usually comprising 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.

Ensuring continuous service in a centralized environment has become fairly straightforward. We know that we need to back up important databases, programs, and documentation, move those backups to recovery sites, and begin processing at that site. However, ISF environments are seldom that centralized; there are usually client-server applications and other distributed applications and connections. For example, a company may be doing business on the Internet and would need to include that application in their continuity plan. Technology Insight 8.3 describes several lessons about ensuring continuous service that were learned as a result of the events of September 11, 2001.

In the spring of 2000, several organizations, including Yahoo!, eBay, CNN.com, and Amazon.com, experienced a serious threat to their ability to ensure continuous service to their customers. The culprit was a relatively new phenomenon, the distributed denial of service attack. Technology Insight 8.4 (page 268) describes these 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. The Yankee Group estimated that the overall cost of these attacks was $1.2 billion. For example, the Yahoo! site was unavailable for three hours, which cost Yahoo! $500,000. Amazon’s site was down for an hour, resulting in a likely loss of $240,000.\(^{10}\)

**Restrict Access to Computing Resources** Can you believe that 90 percent of the respondents to a survey conducted by the Computer Security Institute (CSI) with the participation of the San Francisco Federal Bureau of Investigation’s Computer Intrusion Squad reported security breaches in a recent 12-month period?\(^{11}\)

---

\(^8\) David Essex, “Data Resurrection,” *Computerworld* (March 6, 2000): 76.


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 assure that access to computing resources—systems, data, and programs—is restricted to authorized users for authorized uses by implementing two types of plans:

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

Figure 8.4 (page 269) shows the levels (or layers) of protection included in these two categories.

**Control plans for restricting physical access to computer facilities.** Naturally, only authorized personnel should be allowed access to the computer facility. As shown in the top portion of Figure 8.4, control plans for restricting physical access to computer facilities encompass three layers of controls.

---

**TECHNOLOGY INSIGHT 8.3**

**Business and IT Continuity Lessons Learned as a Result of September 11, 2001**

- Hot sites and cold sites were overwhelmed by the demands for their use by businesses located in and around the WTC. Contracts with these sites must now specify who gets priority for their use.
- Backup and recovery locations must not be located in proximity to the primary site. Some organizations stored their backup data within the WTC complex.
- There must be several post-disaster communication options, including multiple telephone carriers, cell phones, and e-mail. Some telephone and cell phone services were not available in the WTC area for months after the disaster.
- Employees calling in was much more effective than trying to call out to determine the status and location of employees.
- Several organizations, especially those in financial services, realized that they needed their IT resources to be continuously available (i.e., *preventive*) rather than to be recovered after the disaster (i.e., *corrective*).
- Contingency plans must include alternative modes of transportation and should locate recovery sites near where employees live. For several days after 9/11, airlines did not fly, rental cars were hard to find, train and bus systems were severely taxed, and some roads, tunnels, and bridges were closed.
- Paperless offices are only an illusion and back-ups must be created for paper documents using *digital imaging* and other technologies. Organizations lost copies of paper documents and recordings of meetings and legal depositions.

---

**Review Question**

What are the control plans for restricting access to computer facilities? What three “layers” of control do these plans represent? Explain each layer.
Control plans for restricting access to stored programs, data, and documentation.

Control plans for restricting 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 ensure that only authorized users gain access to a system and report violation attempts. These steps are depicted in the lower portion of Figure 8.4.

The primary plans for restricting access in an offline environment involve the use of segregation of duties, restriction of 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. Librarian software can keep track of versions of event and master data and ensure that the correct versions of such data are used. The software can also permit appropriate access to development, testing, staging, and production versions of programs (see Figure 8.3 on page 264).

Ensure Physical Security  To protect IT facilities against manmade 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 events. Table 8.5 (page 270) 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. Even if a malfunction does occur, it is usually detected and corrected automatically. In addition to relying on the controls contained within the com-
Perimeter controls

Building controls

Computer facility controls

Identification

Authentication

Access rights

Threat monitoring

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

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

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 security systems identify authorized personnel through some unique physical trait such as fingers, hands, voice, eyes, face, writing dynamics, and the like.

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.

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
information services, and should see that timely training sessions are conducted. To use IT resources effectively, users often require advice and may require assistance to overcome problems. This assistance is generally delivered via a “help desk” function.

**Monitoring**

Within the monitoring 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 an organizational unit such as the ISF, by an entity’s internal/IT audit group, or by an external organization such as a public accounting or IT consulting firm.

**IT Process 10: Monitor Operations**

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

The WebTrust Seal of Assurance discussed in Chapter 4 is one example of an independent review of IT processes that an organization might obtain. Another service, introduced by the AICPA and the Canadian Institute of Chartered Accountants in 1999, is SysTrust. In a SysTrust engagement, the CA or CPA tests a system to provide assurance that the system meets four criteria (see the qualities of information in Exhibit 1.1 on page 17): availability, security, integrity, and maintainability, while conducting business over the Web.

### Table 8.5 Environmental Controls

<table>
<thead>
<tr>
<th>Environmental hazard</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>Smoke detectors, fire alarms, fire extinguishers, fire-resistant construction materials, insurance</td>
</tr>
<tr>
<td>Water damage</td>
<td>Waterproof ceilings, walls, and floors, adequate drainage, water and moisture detection alarms, insurance</td>
</tr>
<tr>
<td>Dust, coffee, tea, soft drinks</td>
<td>Regular cleaning of rooms and equipment, dust-collecting rugs at entrances, separate dust-generating activities from computer, good housekeeping, prohibiting food and drinks within computing facilities</td>
</tr>
<tr>
<td>Energy increase, decrease, loss</td>
<td>Voltage regulators, backup batteries and generators, fiber optic networks</td>
</tr>
</tbody>
</table>
Similar services to Webtrust and Systrust are offered by many IT consulting and Internet security firms. Check your favorite Web sites to see if they host any “seals of approval” of their transaction security, privacy protection, or system reliability.

Conclusions

Three factors will likely cause managers to confront the issues addressed in this chapter much more directly than have their predecessors. First, the events of September 11, 2001, have changed the way we think about the protecting an organization’s resources, especially its IT resources, and making them available for use. Second, as computer-based systems become more sophisticated, managers must continually question how such technological changes affect the system of internal controls. For example, some companies have already implemented paperless (totally electronic) Information Systems. Others employ electronic data interchange (EDI) technology, which we introduced in Chapter 4. The challenges to managers are to keep pace with the development of such systems, and to ensure that changes in any system are complemented by enhancements in the company’s internal controls.

Third, the events associated with the downfall of companies such as Enron Corp. has heightened the concerns of an organization’s stakeholders—stockholders, customers, employees, taxpayers, etc.—and has caused them to raise a number of corporate (organizational) governance issues. They are asking, for example, how well their board of directors governs its own performance and that of the organization’s management. And, how do the board of directors and management implement and demonstrate that they have control over their business processes? The answers to these questions can be found only in a thorough and effective system of internal control.

RQ8-1 What are the three primary reasons that management exercises control over business processes? Explain.

RQ8-2 What are the relationships between fraud, in general, and internal control? Between computer fraud, in particular, and internal control?

RQ8-3 What is a computer virus?

RQ8-4 Explain what is meant by the control environment. What elements might comprise the control environment?

RQ8-5 Explain how business ethics relates to internal control.

RQ8-6 a. What are the three generic control goals of the operations process and the five generic control goals of the related information process?
b. Explain the difference between the following pairs of control goals: (1) ensure effectiveness of operations and ensure efficient employment of resources; (2) ensure efficient employment of resources and ensure security of resources; (3) ensure input validity and ensure input accuracy; (4) ensure input completeness and ensure input accuracy; (5) ensure input completeness and ensure update completeness; and (6) ensure input accuracy and ensure update accuracy.

RQ8-7  

a. What is the difference between a process control plan, a pervasive control plan, and an IT control process?  
b. Name and describe the five IT resources.  
c. What are the four IT control process domains?

RQ8-8  

What is the purpose of the strategic IT plan?

RQ8-9  

Segregation of duties consists of separating what four basic functions? Briefly define each function.

RQ8-10  

What are personnel control plans? Define the plans.

RQ8-11  

Name and describe the four IT control processes in the acquisition and implementation domain.

RQ8-12  

Describe the four phases/storage locations through which a program under development should pass to ensure good program change control.

RQ8-13  

What is the difference between a hot site and a cold site?

RQ8-14  

What are the control plans for restricting access to computer facilities? What three “layers” of control do these plans represent? Explain each layer.

RQ8-15  

a. What are the control plans for restricting access to stored programs, data, and documentation? Which of these plans apply to an online environment, and which plans apply to an offline environment?  
b. How does a security module work?

RQ8-16  

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?

RQ8-17  

a. Why should an organization conduct monitoring activities?  
b. Who might conduct monitoring activities?
Management is legally responsible for establishing and maintaining an adequate system of control. Discuss the implications of this obligation, and discuss how management discharges its responsibility.

“If it weren’t for the potential of computer abuse, the emphasis on controlling computer systems would decline significantly in importance.” Do you agree? Why or why not?

Provide five examples of potential conflict between the control goals of ensuring effectiveness of operations and of ensuring efficient employment of resources.

“If we thoroughly check the background of every job candidate we want to hire, we’d never get to hire anyone in this tight job market! It just takes too long.” Do you agree? Why or why not?

Discuss the efficiency and effectiveness of the mass-transit system in a large city.

What, if anything, is wrong with the following control hierarchy? Discuss fully.

```
Highest level of control (Pervasive control plans)
  | The control environment
  | Process control plans
Lowest level of control (IT control processes)
```

“In small companies with few employees, it is virtually impossible to implement the segregation of duties control plan.” Do you agree? Why or why not?

“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? Why or why not?

Debate the following point. “Business continuity planning is really an IT issue.”

“Contracting for a standby 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.” Do you agree? Why or why not?

“We use an ASP [Application Service Provider, see Technology Insight 7.1 (page 211)] to outsource all our systems processing. That’s good enough to ensure segregation of duties because we don’t even know who our systems staff is!” Do you agree? Why or why not?

“The ‘monitor operations’ activity in IT process 10 must be performed by an independent function such as a CPA or a security firm.” Do you agree? Why or why not?
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? Why or why not?

DQ8-13

List 1 contains 12 terms from this chapter or from Chapter 1, and list 2 includes 10 definitions or explanations of terms. Match the definitions with the terms by placing a capital letter from list 1 on the blank line to the left of its corresponding definition in list 2. You should have two letters left over from list 1.

A. Process control plan  
B. Control environment  
C. Control goal  
D. Risk  
E. Data maintenance  
F. Master data update  
G. Input accuracy  
H. Input completeness  
I. Input validity  
J. Pervasive control plan  
K. Preventive control plan  
L. Operations process goal

1. The process of modifying master data to reflect the results of new events.
2. A control designed to keep problems from occurring.
3. A control goal of the information process that is directed at ensuring that fictitious or bogus events are not recorded.
4. A goal of an operations process that signifies the very reason for which that system exists.
5. The highest level in the control hierarchy; a control category that evidences management’s commitment to the importance of control in the organization.
6. The process of modifying standing master data.
7. A type of control that is exercised within each business process as that system’s events are processed.
8. The probability that an adverse consequence could result from an organization’s actions or inactions.
9. The element that appears as a heading in each column of a control matrix.
10. A control that addresses a multitude of goals across many business processes.

PROBLEMS

P8-1

List 1 contains 12 terms from this chapter or from Chapter 1, and list 2 includes 10 definitions or explanations of terms. Match the definitions with the terms by placing a capital letter from list 1 on the blank line to the left of its corresponding definition in list 2. You should have two letters left over from list 1.

A. Process control plan  
B. Control environment  
C. Control goal  
D. Risk  
E. Data maintenance  
F. Master data update  
G. Input accuracy  
H. Input completeness  
I. Input validity  
J. Pervasive control plan  
K. Preventive control plan  
L. Operations process goal

1. The process of modifying master data to reflect the results of new events.
2. A control designed to keep problems from occurring.
3. A control goal of the information process that is directed at ensuring that fictitious or bogus events are not recorded.
4. A goal of an operations process that signifies the very reason for which that system exists.
5. The highest level in the control hierarchy; a control category that evidences management’s commitment to the importance of control in the organization.
6. The process of modifying standing master data.
7. A type of control that is exercised within each business process as that system’s events are processed.
8. The probability that an adverse consequence could result from an organization’s actions or inactions.
9. The element that appears as a heading in each column of a control matrix.
10. A control that addresses a multitude of goals across many business processes.

P8-2

Below is a list of eight generic control goals from the chapter, followed by eight descriptions of either system failures (i.e., control goals not met) or instances of successful control plans (i.e., plans that helped to achieve control goals).

List the numbers 1 through 8 on a solution sheet. Each number represents one of the described situations. Next to each number:

a. Place the capital letter of the control goal that best matches the situation described.
b. Provide a one- to two-sentence explanation of how the situation relates to the control goal you selected.

HINT: Some letters may be used more than once. Some letters may not apply at all.

Control Goals

A. Ensure effectiveness of operations.
B. Ensure efficient employment of resources.
C. Ensure security of resources.
D. Ensure input validity.
E. Ensure input completeness.
F. Ensure input accuracy.
G. Ensure update completeness.
H. Ensure update accuracy.

Situations

1. A company uses prenumbered documents for recording its sales invoices to customers. When the invoices for a particular day were entered, the system noted that invoice #12345 appeared twice. The second entry (i.e., the duplicate) of this same number was rejected by the system since it was unsupported by a shipment.

2. In entering the invoices mentioned in situation 1, the data for salesperson number and sales terms were missing from invoice #12349 and therefore were not keyed into the computer.

3. Instead of preparing deposit slips by hand, Causeway Company has them generated by the computer. The company does so in order to speed up the deposit of cash.

4. In the Causeway Company cash receipts system, one of the earliest processes is to endorse each customer’s check with the legend, “for deposit only to Causeway Company.”

5. XYZ Co. prepares customer sales orders on a multipart form, one copy of which is sent to its billing department where it is placed in a temporary file pending shipping notification. Each morning, a billing clerk reviews the file of open sales orders and investigates with the shipping department any missing shipping notices for orders entered 48 hours or more earlier.

6. In situation 5, once a shipping notice is received in the billing department, the first step in preparing the invoice to the customer is to compare the unit prices shown on the sales order with a standard price list kept in the billing system.

7. Alamo Inc. posts its sales invoice event file against its accounts receivable master data each night. Before posting the new sales event data, the computer program first checks the old master data to make sure that it is the version from the preceding day.

8. MiniScribe Corporation recorded actual shipments of disk drives to their warehouse as sales. Those disk drives that had not been ordered by anyone were still the property of MiniScribe.
Part IV  Internal Control for Business Processes and Information Systems

P8-3  In the first list below are 10 examples of the items described in the second list.

Match the two lists by placing the capital letter from the first list on the blank line preceding the description to which it best relates. You should have two letters left over from list 1.

A. Management philosophy and operating style.
B. Customer order received over the Internet.
C. Customer name and address.
D. The process of increasing customer balances for sales made.
E. Total monthly sales report.
F. Fire extinguishers.
G. Deleting an inactive customer’s record from the accounts receivable master data.
H. Ensure input validity.
I. Ensure security of resources.
J. Software piracy.

1. Event data in a computer system.
2. A control goal of the information process.
3. An element included in the control environment.
4. An element of standing data.
5. A control goal of the operations process.
6. An instance of data maintenance.
7. Master data in a computerized system.
8. An illustration of a master data update.

P8-4  Investigate the internal controls in one of the following (ask your instructor which): a local business, your home, your school, or your place of employment. Report (in a manner prescribed by your instructor) on the controls that you found and the goals that they were designed to achieve.

P8-5  Two lists follow. The first is a list of 10 situations that have control implications, and the second is a list of 12 control plans from this chapter.

Control Situations

1. During a violent electrical storm, an employee 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 computer center at Otis Company was badly damaged during a thunderstorm. When they attempted to begin operations at their hot site they discovered that they could not read the tapes containing the backup copies of their data and programs. Apparently, the machines on which the tapes were made had not been operating correctly.
3. Your instructor made arrangements for your class to take a guided tour of the computer center at a large metropolitan bank. The father of one of your classmates had recently been fired as a teller at that bank. That classmate kept his visitor’s badge and gave it to his father, who used it to access the computer center the next day. The father then erased several computer files.
4. The customer service representatives of We-Sell-Everything, 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 order to be completed.

5. At Culpepper Company, most event processing is automated. When an inventory item reaches its reorder point, the computer automatically prints a purchase order for the predetermined economic order quantity (EOQ). Purchase orders of $500 or more require the signature of the purchasing manager; those under $500 are mailed to vendors without being signed. An applications programmer, who was in collusion with the vendor who supplied part 1234, altered the computer program and the inventory master data for that part. He reduced the EOQ and made certain program alterations, such that every time part 1234 reached its reorder point, two purchase orders were produced, each of which was under the $500 threshold.

6. The resume of an applicant for the job of CFO at OYnot Mills showed that the candidate had graduated, some 10 years earlier, magna cum laude from Large State University (LSU) with a major in finance. LSU’s finance program was very well respected, and OYnot had hired several of its graduates over the years. In his second month on the job, the new CFO became tongue-tied when the CEO asked him a technical question about their investment strategy. When later it was discovered that the CFO’s degree from LSU was in mechanical engineering, he was dismissed.

7. June Plugger, the company cashier, was known throughout the company as a workaholic. After three years on the job, June suddenly suffered a gallbladder 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 Deuteronomy Inc. and changed some of the graphics to pornography. Outraged by these changes, some customers took their business elsewhere.

9. During a normal workday, Sydney looked through the trash behind Acme Company’s offices and was able to find some computer reports containing user IDs and other sensitive information. He later used that information to gain access to Acme’s enterprise system.

10. John, an employee at Smith & Company, successfully accessed the order entry system at Smith and entered some orders for goods to be shipped to his cousin at no cost.

Control Plans

A. Personnel termination policies
B. Biometric security systems
C. Personnel selection and hiring control plans
D. Rotation of duties and forced vacations
E. Program change controls
F. Mirror site
G. Service level agreement
Match the 10 situations from the first list with the items in the second list by creating a table similar to the following, and completing column 2, “Control Plan.” In column 2, insert one letter to identify the control plan that would best prevent the system failure from occurring. You should have two letters left over.

<table>
<thead>
<tr>
<th>Control situation</th>
<th>Control plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>___</td>
</tr>
<tr>
<td>2</td>
<td>___</td>
</tr>
<tr>
<td>3</td>
<td>___</td>
</tr>
</tbody>
</table>

Listed here are 20 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:

<table>
<thead>
<tr>
<th>Code</th>
<th>Control Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>___</td>
<td>1. Biometric identification</td>
</tr>
<tr>
<td>___</td>
<td>2. Program change controls</td>
</tr>
<tr>
<td>___</td>
<td>3. Fire and water alarms</td>
</tr>
<tr>
<td>___</td>
<td>4. Adequate fire and water insurance</td>
</tr>
<tr>
<td>___</td>
<td>5. Install batteries to provide backup for temporary loss in power</td>
</tr>
<tr>
<td>___</td>
<td>6. SysTrust examination</td>
</tr>
<tr>
<td>___</td>
<td>7. Service level agreements</td>
</tr>
<tr>
<td>___</td>
<td>8. Chief Privacy Officer</td>
</tr>
<tr>
<td>___</td>
<td>9. Digital signatures</td>
</tr>
<tr>
<td>___</td>
<td>10. Mirror site</td>
</tr>
<tr>
<td>___</td>
<td>11. Rotation of duties and forced vacations</td>
</tr>
<tr>
<td>___</td>
<td>12. Fidelity bonding</td>
</tr>
<tr>
<td>___</td>
<td>13. Hot site</td>
</tr>
<tr>
<td>___</td>
<td>14. Personnel termination policies</td>
</tr>
<tr>
<td>___</td>
<td>15. Segregation of duties</td>
</tr>
<tr>
<td>___</td>
<td>16. IT strategic plan</td>
</tr>
<tr>
<td>___</td>
<td>17. Disaster recovery planning</td>
</tr>
<tr>
<td>___</td>
<td>18. Restrict entry to the computer facility through the use of security guards, locks, badges, and identification cards</td>
</tr>
<tr>
<td>___</td>
<td>19. Computer security module</td>
</tr>
<tr>
<td>___</td>
<td>20. Computer library controls</td>
</tr>
</tbody>
</table>
Two lists follow. The first is a list of 10 situations that have control implications, and the second is a list of 12 control plans from this chapter.

**Situations**

1. A computer programmer was fired for gross incompetence. During the 2-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. It took several months to reconstruct the data from manual source documents and other hardcopy records.
3. A competitor flooded the Oak 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 junior high school computer hacker created a program to generate random telephone numbers and passwords. Over the Web, he used the random number program to “crack” the computer system of a major international corporation.
5. A computer room operator was not able to handle the simplest problems that arose during his shift. He had received all the training recommended for his position and had been counseled a number of times in an attempt to improve his performance.
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 public utility’s computer center overnight and destroyed computer equipment worth several thousand dollars.
8. The computer users at the Barrington Company have experienced significant delays in receiving responses from the computer. They thought that the computer should respond to inquiries in less than three seconds.
9. A disgruntled applications programmer 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.

**Control Plans**

A. Off-site storage of backup computer programs and databases
B. Service level agreements
C. Personnel termination policies
D. Security guards
E. Program change controls
F. Selection and hiring control plans
G. Firewall
H. Batteries and backup generators
I. Help desk
J. Identification badges and visitor’s log
K. Hot site
L. Security modules

Match the 10 situations from the first list with the items in the two other lists by making a table like that shown for Problem 1. In column 2, insert one letter to identify the control plan that would best prevent the system failure from occurring. You should have two letters left over.

**P8-8**

Assume that inventory records are kept in an enterprise system and that the options in the inventory system module are as follows:

1. Maintain inventory master data (i.e., add new products, change or delete old products in the inventory master data).
2. Record newly arrived shipments of inventory.
3. Record returns of incorrect or damaged inventory.
4. Select items to be reordered, the amount to reorder, and the vendor.
5. Print and record new orders.
6. Print inventory reports.

Further assume that personnel in the inventory 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 table below, show which users should (or should not) have access to each of the six accounts payable options. Make and state whatever assumptions you think are necessary. Explain in one or two paragraphs how your matrix design would optimize the segregation of duties control plan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Manager</th>
<th>Romeo</th>
<th>Juliet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

**P8-9**

Conduct research on the events related to the Enron Corp. bankruptcy in December 2001. Prepare a report describing the controls that might have prevented, detected, or corrected the stakeholder losses associated with that bankruptcy.

**P8-10**

Conduct research on the events related to the disasters of September 11, 2001. Prepare a report describing the controls that might have prevented, detected, or corrected the losses suffered by companies in the World Trade Center.