Chapter 7

Control and Accounting Information Systems

Learning Objectives

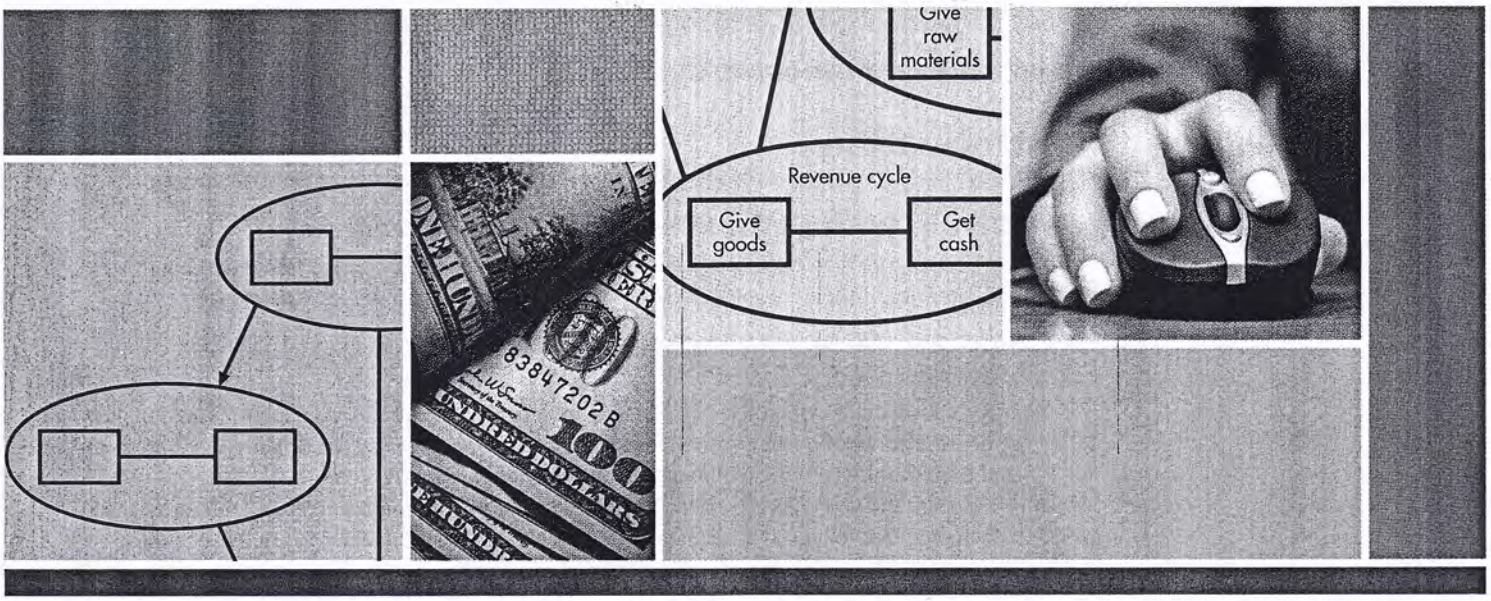
After studying this chapter, you should be able to:

1. Explain basic control concepts and explain why computer control and security are important.
2. Compare and contrast the COBIT, COSO, and ERM control frameworks.
3. Describe the major elements in the internal environment of a company.
4. Describe the four types of control objectives that companies need to set.
5. Describe the events that affect uncertainty and the techniques used to identify them.
6. Explain how to assess and respond to risk using the Enterprise Risk Management (ERM) model.
7. Describe control activities commonly used in companies.
8. Describe how to communicate information and monitor control processes in organizations.

INTEGRATIVE CASE SPRINGER'S LUMBER & SUPPLY

Jason Scott, an internal auditor for Northwest Industries, is auditing Springer's Lumber & Supply, Northwest's building materials outlet in Bozeman, Montana. His supervisor, Maria Pilier, asked him to trace a sample of purchase transactions from purchase requisition to cash disbursement to verify that proper control procedures were followed. Jason is frustrated with this task, and for good reasons:

- The purchasing system is poorly documented.
- He keeps finding transactions that have not been processed as Ed Yates, the accounts payable manager, said they should be.



- Purchase requisitions are missing for several items personally authorized by Bill Springer, the purchasing vice president.
- Some vendor invoices have been paid without supporting documents, such as purchase orders and receiving reports.
- Prices for some items seem unusually high, and there are a few discrepancies in item prices between the vendor invoice and the corresponding purchase order.

Yates had a logical answer for every question Jason raised and advised Jason that the real world is not as tidy as the world portrayed in college textbooks. Maria also has some concerns:

- Springer's is the largest supplier in the area and has a near monopoly.
- Management authority is held by the company president, Joe Springer, and his two sons, Bill (the purchasing vice president) and Ted (the controller). Several relatives and friends are on the payroll. Together, the Springers own 10% of the company.
- Lines of authority and responsibility within the company are loosely defined and confusing.
- Maria believes that Ted Springer may have engaged in "creative accounting" to make Springer's one of Northwest's best-performing retail outlets.

After talking to Maria, Jason ponders the following issues:

1. Because Ed Yates had a logical explanation for every unusual transaction, should Jason describe these transactions in his report?
2. Is a violation of control procedures acceptable if management has authorized it?
3. Maria's concerns about Springer's loosely defined lines of authority and possible use of "creative accounting" are matters of management policy. With respect to Jason's control procedures assignment, does he have a professional or an ethical responsibility to get involved?

Introduction

Why Threats to Accounting Information Systems Are Increasing

In most years, more than 60% of organizations experience a major failure in controlling the security and integrity of their computer systems. Reasons for the failures include the following:

- Information is available to an unprecedented number of workers. Chevron, for example, has over 35,000 PCs.
- Information on distributed computer networks is hard to control. At Chevron, information is distributed among many systems and thousands of employees worldwide. Each system and each employee represent a potential control vulnerability point.
- Customers and suppliers have access to each others' systems and data. For example, WalMart allows vendors to access their databases. Imagine the confidentiality problems as these vendors form alliances with WalMart competitors.

Organizations have not adequately protected data for several reasons:

- Some companies view the loss of crucial information as a distant, unlikely threat.
- The control implications of moving from centralized computer systems to Internet-based systems are not fully understood.
- Many companies do not realize that information is a strategic resource and that protecting it must be a strategic requirement. For example, one company lost millions of dollars because it did not protect data transmissions. A competitor tapped into its phone lines and obtained faxes of new product designs.
- Productivity and cost pressures motivate management to forgo time-consuming control measures.

Any potential adverse occurrence is called a ***threat*** or an event. The potential dollar loss from a threat is called the ***exposure*** or ***impact.*** The probability that it will happen is called the ***likelihood*** of the threat.

Overview of Control Concepts

Internal control is the process implemented to provide reasonable assurance that the following control objectives are achieved:

- Safeguard assets: prevent or detect their unauthorized acquisition, use, or disposition.
- Maintain records in sufficient detail to report company assets accurately and fairly.
- Provide accurate and reliable information.
- Prepare financial reports in accordance with established criteria.
- Promote and improve operational efficiency.
- Encourage adherence to prescribed managerial policies.
- Comply with applicable laws and regulations.

Internal control is a process because it permeates an organization's operating activities and is an integral part of management activities. Internal control provides reasonable assurance—complete assurance is difficult to achieve and prohibitively expensive. In addition, internal control systems have inherent limitations, such as susceptibility to simple errors and mistakes, faulty judgments and decision making, management overrides, and collusion.

Developing an internal control system requires a thorough understanding of information technology (IT) capabilities and risks, as well as how to use IT to achieve an organization's control objectives. Accountants and systems developers help management achieve their control objectives by (1) designing effective control systems that take a proactive approach to eliminating system threats and that detect, correct, and recover from threats when they occur; and (2) making it easier to build controls into a system at the initial design stage than to add them after the fact.

Internal controls perform three important functions:

1. ***Preventive controls*** deter problems before they arise. Examples include hiring qualified personnel, segregating employee duties, and controlling physical access to assets and information.
2. ***Detective controls*** discover problems that are not prevented. Examples include duplicate checking of calculations and preparing bank reconciliations and monthly trial balances.
3. ***Corrective controls*** identify and correct problems as well as correct and recover from the resulting errors. Examples include maintaining backup copies of files, correcting data entry errors, and resubmitting transactions for subsequent processing.

Internal controls are often segregated into two categories:

1. ***General controls*** make sure an organization's control environment is stable and well managed. Examples include security; IT infrastructure; and software acquisition, development, and maintenance controls.
2. ***Application controls*** make sure transactions are processed correctly. They are concerned with the accuracy, completeness, validity, and authorization of the data captured, entered, processed, stored, transmitted to other systems, and reported.

Robert Simons, a Harvard business professor, has espoused four levels of control to help management reconcile the conflict between creativity and controls.

1. A ***belief system*** describes how the company creates value, helps employees understand management's vision, communicates company core values, and inspires employees to live by those values.
2. A ***boundary system*** helps employees act ethically by setting boundaries on employee behavior. Employees are not told exactly what to do. Instead, they are encouraged to creatively solve problems and meet customer needs while meeting minimum performance standards, shunning off-limit activities, and avoiding actions that might damage their reputation.
3. A ***diagnostic control system*** measures, monitors, and compares actual company progress to budgets and performance goals. Feedback helps management adjust and fine-tune inputs and processes so future outputs more closely match goals.
4. An ***interactive control system*** helps managers to focus subordinates' attention on key strategic issues and to be more involved in their decisions. Interactive system data are interpreted and discussed in face-to-face meetings of superiors, subordinates, and peers.

Regrettably, not all organizations have an effective internal control system. For instance, one report indicated that the FBI is plagued by IT infrastructure vulnerabilities and security problems, some of which were identified in an audit 13 years previously. Specific areas of concern were security standards, guidelines, and procedures; segregation of duties; access controls, including password management and usage; backup and recovery controls; and software development and change controls.

The Foreign Corrupt Practices and Sarbanes–Oxley Acts

In 1977, the *Foreign Corrupt Practices Act (FCPA)* was passed to prevent companies from bribing foreign officials to obtain business. Congress incorporated language from an American Institute of Certified Public Accountants (AICPA) pronouncement into the FCPA that required corporations to maintain good systems of internal control. Unfortunately, these requirements were not sufficient to prevent further problems.

In the late 1990s and early 2000s, news stories were reporting accounting frauds at Enron, WorldCom, Xerox, Tyco, Global Crossing, Adelphia, and other companies. When Enron, with $62 billion in assets, declared bankruptcy in December 2001, it was the largest bankruptcy in U.S. history. In June 2002, Arthur Andersen, once the largest CPA firm, collapsed. The Enron bankruptcy was dwarfed when WorldCom, with over $100 billion in assets, filed for bankruptcy in July 2002. In response to these frauds, Congress passed the *Sarbanes–Oxley Act (SOX)* of 2002. SOX applies to publicly held companies and their auditors and was designed to prevent financial statement fraud, make financial reports more transparent, protect investors, strengthen internal controls, and punish executives who perpetrate fraud.

SOX is the most important business-oriented legislation in the last 75 years. It changed the way boards of directors and management operate and had a dramatic impact on CPAs who audit them. The following are some of the most important aspects of SOX:

- *Public Company Accounting Oversight Board (PCAOB).* SOX created the ***Public Company Accounting Oversight Board (PCAOB)*** to control the auditing profession. The PCAOB sets and enforces auditing, quality control, ethics, independence, and other auditing standards.
- *New rules for auditors.* Auditors must report specific information to the company's audit committee, such as critical accounting policies and practices. Audit partners must be rotated periodically. SOX prohibits auditors from performing certain nonaudit services, such as information systems design and implementation. Audit firms cannot provide services to companies if top management was employed by the auditing firm and worked on the company's audit in the preceding 12 months.
- *New roles for audit committees.* Audit committee members must be on the company's board of directors and be independent of the company. One member of the audit committee must be a financial expert. The audit committee hires, compensates, and oversees the auditors, who report directly to them.
- *New rules for management.* SOX requires the CEO and CFO to certify that (1) financial statements and disclosures are fairly presented, were reviewed by management, and are not misleading; and that (2) the auditors were told about all material internal control weaknesses and fraud. If management knowingly violates these rules, they can be prosecuted and fined. Companies must disclose, in plain English, material changes to their financial condition on a timely basis.
- *New internal control requirements.* Section 404 requires companies to issue a report accompanying the financial statements stating that management is responsible for establishing and maintaining an adequate internal control system. The report must contain management's assessment of the company's internal controls, attest to their accuracy, and report significant weaknesses or material noncompliance.

After SOX was passed, the SEC mandated that management must:

- Base its evaluation on a recognized control framework. The most likely frameworks, formulated by COSO, are discussed in this chapter.
- Disclose all material internal control weaknesses.
- Conclude that a company does not have effective financial reporting internal controls if there are material weaknesses.

Control Frameworks

This section discusses three frameworks used to develop internal control systems.

COBIT Framework

The Information Systems Audit and Control Association (ISACA) developed the ***Control Objectives for Information and Related Technology (COBIT)*** framework. COBIT consolidates control standards from 36 different sources into a single framework that allows (1) management to benchmark security and control practices of IT environments, (2) users to be assured that adequate IT security and control exist, and (3) auditors to substantiate their internal control opinions and to advise on IT security and control matters.

The framework addresses control from three vantage points:

1. *Business objectives.* To satisfy business objectives, information must conform to seven categories of criteria that map into the objectives established by the Committee of Sponsoring Organizations (COSO; see next section).
2. *IT resources.* These include people, application systems, technology, facilities, and data.
3. *IT processes.* These are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring and evaluation.

The COBIT framework is shown in Figure 8-1 and discussed in more depth in Chapters 8 through 10.

COSO's Internal Control Framework

The *Committee of Sponsoring Organizations (COSO)* consists of the American Accounting Association, the American Institute of Certified Public Accountants, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute. In 1992, COSO issued *Internal Control—Integrated Framework (IC)*, which is widely accepted as the authority on internal controls and is incorporated into policies, rules, and regulations used to control business activities.

The five components of the IC framework, summarized in Table 7-1, are part of COSO's newer Enterprise Risk Management framework.

COSO's Enterprise Risk Management Framework

To improve the risk management process, COSO developed a second control framework called *Enterprise Risk Management—Integrated Framework (ERM)*. ERM is the process the board of directors and management use to set strategy, identify events that may affect the entity, assess and manage risk, and provide reasonable assurance that the company achieves its objectives and goals. The basic principles behind ERM are as follows:

- Companies are formed to create value for their owners.
- Management must decide how much uncertainty it will accept as it creates value.
- Uncertainty results in risk, which is the possibility that something negatively affects the company's ability to create or preserve value.
- Uncertainty results in opportunity, which is the possibility that something positively affects the company's ability to create or preserve value.
- The ERM framework can manage uncertainty as well as create and preserve value.

COSO developed Figure 7-1 to illustrate the elements of ERM. The four columns at the top represent the objectives management must meet to achieve company goals. The columns on the right represent the company's units. The horizontal rows are the eight interrelated risk and control components of ERM. The ERM model is three-dimensional. Each of the eight risk and control elements applies to each of the four objectives and to the company and/or one of its subunits. For example, XYZ Company could look at the control activities for the operations objectives in its Pacific Division.

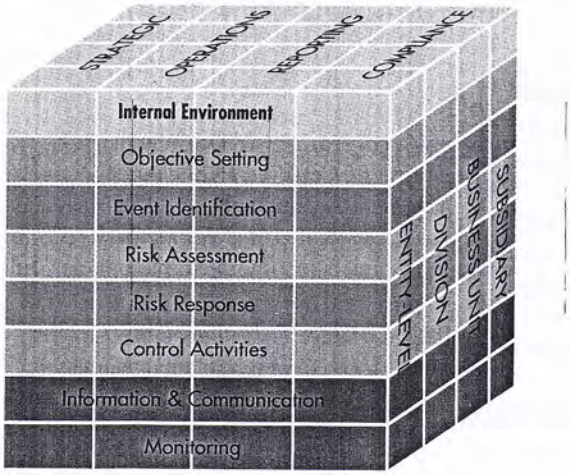
The Enterprise Risk Management Framework versus the Internal Control Framework

The IC framework has been widely adopted as the way to evaluate internal controls, as required by Sarbanes–Oxley. However, it examines controls without looking at the purposes and risks of business processes and provides little context for evaluating the results. Under the IC framework,

TABLE 7-1 Five Interrelated Components of COSO's Internal Control Model

Component	Description
Control environment	The core of any business is its people—their individual attributes, including integrity, ethical values, and competence—and the environment in which they operate. They are the engine that drives the organization and the foundation on which everything rests.
Control activities	Control policies and procedures help ensure that the actions identified by management as necessary to address risks and achieve the organization's objectives are effectively carried out.
Risk assessment	The organization must identify, analyze, and manage its risks. It must set objectives so that the organization is operating in concert.
Information and communication	Information and communication systems capture and exchange the information needed to conduct, manage, and control the organization's operations.
Monitoring	The entire process must be monitored, and modifications made as necessary so the system can change as conditions warrant.

FIGURE 7-1
COSO's Enterprise Risk Management Model



it is hard to know which control systems are most important, whether they adequately deal with risk, and whether important controls are missing.

The more comprehensive ERM framework takes a risk-based rather than a controls-based approach. ERM adds three additional elements to COSO's IC framework: setting objectives, identifying events that may affect the company, and developing a response to assessed risk. As a result, controls are flexible and relevant because they are linked to current organizational objectives. The ERM model also recognizes that risk, in addition to being controlled, can be accepted, avoided, diversified, shared, or transferred.

Because it is more comprehensive, the ERM model will likely become the more widely adopted model. The eight ERM components shown in Figure 7-1 are the topic of the remainder of the chapter.

The Internal Environment

The ***internal environment***, or company culture, influences how organizations establish strategies and objectives; structure business activities; and identify, assess, and respond to risk. It is the foundation for all other ERM components. A weak or deficient internal environment often results in breakdowns in risk management and control. It is essentially the same thing as the control environment in the IC framework.

An internal environment consists of the following:

1. Management's philosophy, operating style, and risk appetite
2. The board of directors
3. Commitment to integrity, ethical values, and competence
4. Organizational structure
5. Methods of assigning authority and responsibility
6. Human resource standards
7. External influences

Enron is an example of an ineffective internal environment that resulted in financial failure. Although Enron appeared to have an effective ERM system, its internal environment was defective. Management engaged in risky and dubious business practices, which the board of directors never questioned. Management misrepresented the company's financial condition, lost the confidence of shareholders, and finally filed for bankruptcy.

Management's Philosophy, Operating Style, and Risk Appetite

Collectively, an organization has a philosophy, or shared beliefs and attitudes, about risk that affects policies, procedures, oral and written communications, and decisions. Companies also

have a ***risk appetite***, which is the amount of risk they are willing to accept to achieve their goals. To avoid undue risk, risk appetite must be in alignment with company strategy.

The more responsible management's philosophy and operating style, and the more clearly they are communicated, the more likely employees will behave responsibly. If management has little concern for internal controls and risk management, then employees are less diligent in achieving control objectives. The culture at Springer's Lumber & Supply provides an example. Maria Pilier found that lines of authority and responsibility were loosely defined and suspected management might have used "creative accounting" to improve company performance. Jason Scott found evidence of poor internal control practices in the purchasing and accounts payable functions. These two conditions may be related; management's loose attitude may have contributed to the purchasing department's inattentiveness to good internal control practices.

Management's philosophy, operating style, and risk appetite can be assessed by answering questions such as these:

- Does management take undue business risks to achieve its objectives, or does it assess potential risks and rewards prior to acting?
- Does management manipulate performance measures, such as net income, so they are seen in a more favorable light?
- Does management pressure employees to achieve results regardless of the methods, or does it demand ethical behavior? In other words, do the ends justify the means?

The Board of Directors

An involved board of directors represents shareholders and provides an independent review of management that acts as a check and balance on its actions. Sarbanes–Oxley requires public companies to have an ***audit committee*** of outside, independent directors. The audit committee is responsible for financial reporting, regulatory compliance, internal control, and hiring and overseeing internal and external auditors, who report all critical accounting policies and practices to them. Directors should also approve company strategy and review security policies.

Commitment to Integrity, Ethical Values, and Competence

Organizations need a culture that stresses integrity and commitment to ethical values and competence. Ethics pays—ethical standards are good business. Integrity starts at the top, as company employees adopt top management attitudes about risks and controls. A powerful message is sent when the CEO, confronted with a difficult decision, makes the ethically correct choice.

Companies endorse integrity by:

- Actively teaching and requiring it—for example, making it clear that honest reports are more important than favorable ones.
- Avoiding unrealistic expectations or incentives that motivate dishonest or illegal acts, such as overly aggressive sales practices, unfair or unethical negotiation tactics, and bonuses excessively based on reported financial results.
- Consistently rewarding honesty and giving verbal labels to honest and dishonest behavior. If companies punish or reward honesty without labeling it as such, or if the standard of honesty is inconsistent, then employees will display inconsistent moral behavior.
- Developing a written code of conduct that explicitly describes honest and dishonest behaviors. For example, most purchasing agents agree that accepting $5,000 from a supplier is dishonest, but a weekend vacation is not as clear-cut. A major cause of dishonesty comes from rationalizing unclear situations and allowing the criterion of expediency to replace the criterion of right versus wrong. Companies should document that employees have read and understand the code of conduct.
- Requiring employees to report dishonest or illegal acts and disciplining employees who knowingly fail to report them. All dishonest acts should be investigated, and dishonest employees should be dismissed and prosecuted to show that such behavior is not allowed.
- Making a commitment to competence. Companies should hire competent employees with the necessary knowledge, experience, training, and skills.

Organizational Structure

A company's organizational structure provides a framework for planning, executing, controlling, and monitoring operations. Important aspects of the organizational structure include the following:

- Centralization or decentralization of authority
- A direct or matrix reporting relationship
- Organization by industry, product line, location, or marketing network
- How allocation of responsibility affects information requirements
- Organization of and lines of authority for accounting, auditing, and information system functions
- Size and nature of company activities

A complex or unclear organizational structure may indicate serious problems. For example, ESM, a brokerage company, used a multilayered organizational structure to hide a $300 million fraud. Management hid stolen cash in their financial statements using a fictitious receivable from a related company.

In today's business world, hierarchical structures, with layers of management who supervise others, are being replaced with flat organizations of self-directed work teams that make decisions without needing multiple layers of approval. The emphasis is on continuous improvement rather than periodic reviews and appraisals. These organizational structure changes impact the nature and type of controls used.

Methods of Assigning Authority and Responsibility

Management should make sure employees understand entity goals and objectives, assign authority and responsibility for them to departments and individuals, hold them accountable for achieving them, and encourage the use of initiative to solve problems. It is especially important to identify who is responsible for the company's information security policy.

Authority and responsibility are assigned and communicated using formal job descriptions, employee training, operating schedules, budgets, a code of conduct, and written policies and procedures. The ***policy and procedures manual*** explains proper business practices, describes needed knowledge and experience, explains document procedures, explains how to handle transactions, and lists the resources provided to carry out specific duties. The manual includes the chart of accounts and copies of forms and documents. It is a helpful on-the-job reference for current employees and a useful tool for training new employees.

Human Resources Standards

One of the greatest control strengths is the honesty of employees; one of the greatest control weaknesses is the dishonesty of employees. Human resource policies and practices governing working conditions, job incentives, and career advancement can be a powerful force in encouraging honesty, efficiency, and loyal service. Policies should convey the required level of expertise, competence, ethical behavior, and integrity required. The following policies and procedures are important.

HIRING Employees should be hired based on educational background, experience, achievements, honesty and integrity, and meeting written job requirements. All company personnel, including cleaning crews and temporary employees, should be subject to hiring policies. Some fraudsters pose as janitors or temporary employees to gain physical access to company computers.

Applicant qualifications can be evaluated using resumes, reference letters, interviews, and background checks. A thorough ***background check*** includes talking to references, checking for a criminal record, examining credit records, and verifying education and work experience. Many applicants include false information in their applications or resumes. Philip Crosby Associates (PCA) hired John Nelson, MBA, CPA, without conducting a background check. In reality, the CPA designation and his glowing references were phony. Nelson was actually Robert W. Liszewski, who had served an 18-month jail sentence for embezzling $400,000. By the time PCA discovered this, Liszewski had embezzled $960,000 using wire transfers to a dummy corporation, supported by forged signatures on contracts and authorization documents.

Many firms hire companies that specialize in background checks because some applicants buy phony degrees from Web site operators who "validate" the bogus education when employers

call. Some applicants even pay hackers to break into university databases and enter fake graduation or grade data.

Compensating, Evaluating and Promoting Poorly compensated employees are more likely to feel resentment and financial pressures that can motivate fraud. Fair pay and appropriate bonus incentives help motivate and reinforce outstanding employee performance. Employees should be given periodic performance appraisals to help them understand their strengths and weaknesses. Promotions should be based on performance and qualifications.

TRAINING Training programs should teach new employees their responsibilities; expected levels of performance and behavior; and the company's policies and procedures, culture, and operating style. Employees can be trained by conducting informal discussions and formal meetings, issuing periodic memos, distributing written guidelines and codes of professional ethics, circulating reports of unethical behavior and its consequences, and promoting security and fraud training programs. Ongoing training helps employees tackle new challenges, stay ahead of the competition, adapt to changing technologies, and deal effectively with the evolving environment.

Fraud is less likely to occur when employees believe security is everyone's business, are proud of their company and protective of its assets, and recognize the need to report fraud. Such a culture has to be created, taught, and practiced. Acceptable and unacceptable behavior should be defined. Many computer professionals see nothing wrong with using corporate computer resources to gain unauthorized access to databases and browse them. The consequences of unethical behavior (reprimands, dismissal, and prosecution) should also be taught and reinforced.

MANAGING DISGRUNTLED EMPLOYEES Some disgruntled employees, seeking revenge for a perceived wrong, perpetrate fraud or sabotage systems. Companies need procedures to identify disgruntled employees and either help them resolve their feelings or remove them from sensitive jobs. For example, a company may choose to establish grievance channels and provide employee counseling. Helping employees resolve their problems is not easy to do, however, because most employees fear that airing their feelings could have negative consequences.

DISCHARGING Dismissed employees should be removed from sensitive jobs immediately and denied access to the information system. One terminated employee lit a butane lighter under a smoke detector located just outside the computer room. It set off a sprinkler system that ruined most of the computer hardware.

VACATIONS AND ROTATION OF DUTIES Fraud schemes that require ongoing perpetrator attention are uncovered when the perpetrator takes time off. Periodically rotating employee duties and making employees take vacations can achieve the same results. For example, the FBI raided a gambling establishment and discovered that Roswell Steffen, who earned $11,000 a year, was betting $30,000 a day at the racetrack. The bank where he worked discovered that he embezzled and gambled away $1.5 million over a three-year period. A compulsive gambler, Steffen borrowed $5,000 to bet on a "sure thing" that did not pan out. He embezzled ever-increasing amounts in an effort to win back the money he had "borrowed." Steffen's scheme was simple; he transferred money from inactive accounts to his own account. If anyone complained, Steffen, the chief teller with the power to resolve these types of problems, replaced the money by taking it from another inactive account. When asked, after his arrest, how the fraud could have been prevented, Steffen said the bank could have coupled a two-week vacation with several weeks of rotation to another job function. Had the bank taken these measures, Steffen's embezzlement, which required his physical presence at the bank, would have been almost impossible to cover up.

CONFIDENTIALITY AGREEMENTS AND FIDELITY BOND INSURANCE All employees, suppliers, and contractors should sign and abide by a confidentiality agreement. Fidelity bond insurance coverage of key employees protects companies against losses arising from deliberate acts of fraud.

PROSECUTE AND INCARCERATE PERPETRATORS Most fraud is not reported or prosecuted for several reasons:

1. Companies are reluctant to report fraud because it can be a public relations disaster. The disclosure can also reveal system vulnerabilities and attract more fraud or hacker attacks.
2. Law enforcement and the courts are busy with violent crimes and have less time and interest for computer crimes in which no physical harm occurs.

3. Fraud is difficult, costly, and time-consuming to investigate and prosecute.
4. Many law enforcement officials, lawyers, and judges lack the computer skills needed to investigate and prosecute computer crimes.
5. Fraud sentences are often light. A famous example involved C. Arnold Smith, former owner of the San Diego Padres, who was named Mr. San Diego of the Century. Smith was involved in the community and made large political contributions. When investigators discovered he had stolen $200 million from his bank, he pleaded no contest. His sentence was four years of probation. He was fined $30,000, to be paid at the rate of $100 a month for 25 years with no interest. Mr. Smith was 71 at the time. The embezzled money was never recovered.

External Influences

External influences include requirements imposed by stock exchanges, the Financial Accounting Standards Board (FASB), the Public Company Accounting Oversight Board (PCAOB), and the Securities and Exchange Commission (SEC). They also include requirements imposed by regulatory agencies, such as those for banks, utilities, and insurance companies.

Objective Setting

Objective setting is the second ERM component. Management determines what the company hopes to achieve, often referred to as the *corporate* vision or mission. Management sets objectives at the corporate level and then subdivides them into more specific objectives for company subunits. The company determines what must go right to achieve the objectives and establishes performance measures to determine whether they are met.

Strategic objectives, which are high-level goals that are aligned with the company's mission, support it, and create shareholder value, are set first. Management should identify alternative ways of accomplishing the strategic objectives; identify and assess the risks and implications of each alternative; formulate a corporate strategy; and set operations, compliance, and reporting objectives.

Operations objectives, which deal with the effectiveness and efficiency of company operations, determine how to allocate resources. They reflect management preferences, judgments, and style and are a key factor in corporate success. They vary significantly—one company may decide to be an early adopter of technology, another may adopt technology when it is proven, and a third may adopt it only after it is generally accepted.

Reporting objectives help ensure the accuracy, completeness, and reliability of company reports; improve decision making; and monitor company activities and performance. ***Compliance objectives*** help the company comply with all applicable laws and regulations. Most compliance objectives, and many reporting objectives, are imposed by external entities in response to laws or regulations. How well a company meets its compliance and reporting objectives can significantly impact a company's reputation.

ERM provides reasonable assurance that reporting and compliance objectives are achieved because companies have control over them. However, the only reasonable assurance ERM can provide about strategic and operations objectives, which are sometimes at the mercy of uncontrollable external events, is that management and directors are informed on a timely basis of the progress the company is making in achieving them.

Event Identification

COSO defines an ***event*** as "an incident or occurrence emanating from internal or external sources that affects implementation of strategy or achievement of objectives. Events may have positive or negative impacts or both." An event represents uncertainty; it may or may not occur. If it does occur, it is hard to know when. Until it occurs, it may be difficult to determine its

impact. When it occurs, it may trigger another event. Events may occur individually or concurrently. Management must try to anticipate all possible positive or negative events, determine which are most and least likely to occur, and understand the interrelationship of events.

As an example, consider the implementation of an electronic data interchange (EDI) system that creates electronic documents, transmits them to customers and suppliers, and receives electronic responses in return. A few of the events a company could face are choosing an inappropriate technology, unauthorized access, loss of data integrity, incomplete transactions, system failures, and incompatible systems.

Some techniques companies use to identify events include using a comprehensive list of potential events, performing an internal analysis, monitoring leading events and trigger points, conducting workshops and interviews, using data mining, and analyzing business processes.

Risk Assessment and Risk Response

The risks of an identified event are assessed in several different ways: likelihood, positive and negative impacts, individually and by category, their effect on other organizational units, and on an inherent and a residual basis. ***Inherent risk*** exists before management takes any steps to control the likelihood or impact of an event. ***Residual risk*** is what remains after management implements internal controls or some other response to risk. Companies should assess inherent risk, develop a response, and then assess residual risk.

To align identified risks with the company's tolerance for risk, management must take an entity-wide view of risk. They assess a risk's likelihood and impact, as well as the costs and benefits of the alternative responses. Management can respond to risk in one of four ways:

- *Reduce.* Reduce the likelihood and impact of risk by implementing an effective system of internal controls.
- *Accept.* Accept the likelihood and impact of the risk.
- *Share.* Share risk or transfer it to someone else by buying insurance, outsourcing an activity, or entering into hedging transactions.
- *Avoid.* Avoid risk by not engaging in the activity that produces the risk. This may require the company to sell a division, exit a product line, or not expand as anticipated.

Accountants and systems designers help management design effective control systems to reduce inherent risk. They also evaluate internal control systems to ensure that they are operating effectively. They assess and reduce inherent risk using the risk assessment and response strategy shown in Figure 7-2. The first step, event identification, has already been discussed.

Estimate Likelihood and Impact

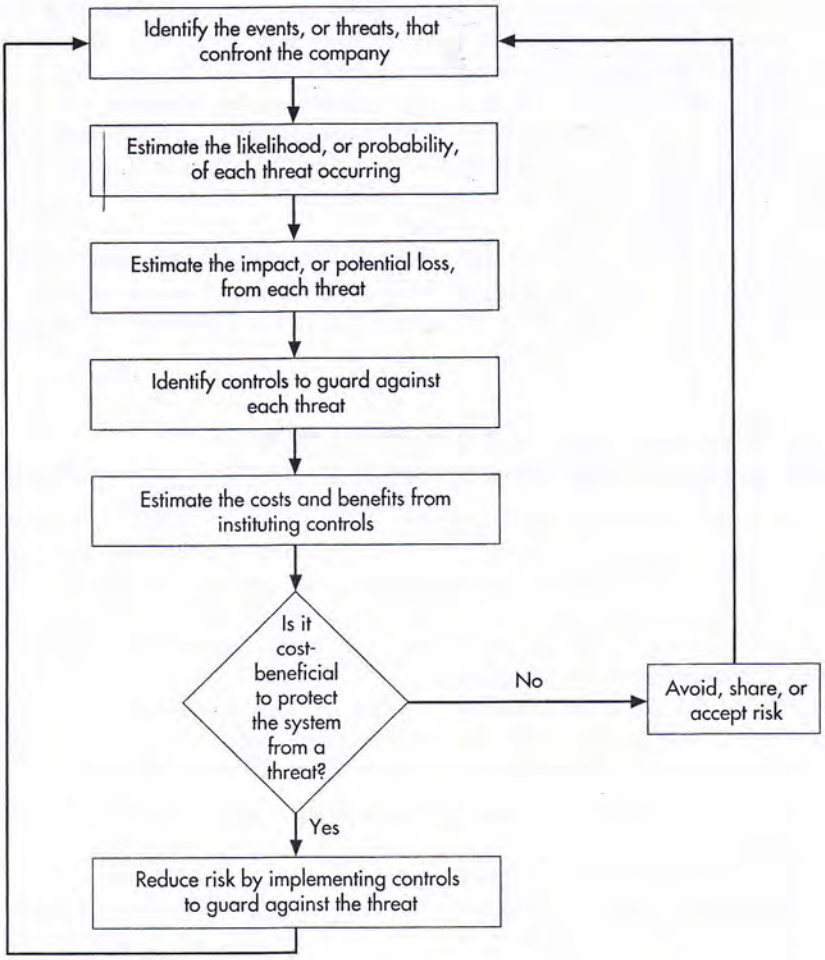
Some events pose a greater risk because they are more likely to occur. Employees are more likely to make a mistake than to commit fraud, and a company is more likely to be the victim of a fraud than an earthquake. The likelihood of an earthquake may be small, but its impact could destroy a company. The impact of fraud is usually not as great, because most instances of fraud do not threaten a company's existence. Likelihood and impact must be considered together. As either increases, both the materiality of the event and the need to protect against it rise.

Software tools help automate risk assessment and response. Blue Cross Blue Shield of Florida uses ERM software that lets managers enter perceived risks; assess their nature, likelihood, and impact; and assign them a numerical rating. An overall corporate assessment of risk is developed by aggregating all the rankings.

Identify Controls

Management should identify controls that protect the company from each event. Preventive controls are usually superior to detective controls. When preventive controls fail, detective controls are essential for discovering the problem. Corrective controls help recover from any problems. A good internal control system should employ all three.

FIGURE 7-2
Risk Assessment Approach to Designing Internal Controls



Estimate Costs and Benefits

The objective in designing an internal control system is to provide reasonable assurance that events do not take place. No internal control system provides foolproof protection against all events, because having too many controls is cost-prohibitive and negatively affects operational efficiency. Conversely, having too few controls will not provide the needed reasonable assurance.

The benefits of an internal control procedure must exceed its costs. Benefits, which can be hard to quantify accurately, include increased sales and productivity, reduced losses, better integration with customers and suppliers, increased customer loyalty, competitive advantages, and lower insurance premiums. Costs are usually easier to measure than benefits. A primary cost element is personnel, including the time to perform control procedures, the costs of hiring additional employees to achieve effective segregation of duties, and the costs of programming controls into a computer system.

One way to estimate the value of internal controls involves ***expected loss***, the mathematical product of impact and likelihood:

$$\text{Expected loss} = \text{Impact} \times \text{Likelihood}$$

The value of a control procedure is the difference between the expected loss with the control procedure(s) and the expected loss without it.

Determine Cost/Benefit Effectiveness

Management should determine whether a control is cost beneficial. For example, at Atlantic Richfield data errors occasionally required an entire payroll to be reprocessed, at a cost of $10,000. A data validation step would reduce the event likelihood from 15% to 1%, at a cost of $600 per pay period. The cost/benefit analysis that determined that the validation step should be employed is shown in Table 7-2.

TABLE 7-2 Cost/Benefit Analysis of Payroll Validation Procedure

	Without Validation Procedure	With Validation Procedure	Net Expected Difference
Cost to reprocess entire payroll	$10,000	$10,000	
Likelihood of payroll data errors	15%	1%	
Expected reprocessing cost ($10,000 ×likelihood)	$1,500	$100	$1,400
Cost of validation procedure	$0	$600	$(600)
Net expected benefit of validation procedure			$800

In evaluating internal controls, management must consider factors other than those in the expected benefit calculation. For example, if an event threatens an organization's existence, its extra cost can be viewed as a catastrophic loss insurance premium.

Implement Control or Accept, Share, or Avoid the Risk

Cost-effective controls should be implemented to reduce risk. Risks not reduced must be accepted, shared, or avoided. Risk can be accepted if it is within the company's risk tolerance range. An example is a risk with a small likelihood and a small impact. A response to reduce or share risk helps bring residual risk into an acceptable risk tolerance range. A company may choose to avoid the risk when there is no cost-effective way to bring risk into an acceptable risk tolerance range.

Control Activities

Control activities are policies and procedures that provide reasonable assurance that control objectives are met and risk responses are carried out. It is management's responsibility to develop a secure and adequately controlled system. Management establishes a set of procedures to ensure control compliance and enforcement. The information security officer and the operations staff are responsible for ensuring that control procedures are followed.

Controls are much more effective when placed in the system as it is built, rather than as an afterthought. As a result, managers need to involve systems analysts, designers, and end users when designing computer-based control systems. It is important that control activities be in place during the end-of-the-year holiday season, because a disproportionate amount of computer fraud and security break-ins takes place during this time. Some reasons for this are (1) extended employee vacations mean that there fewer people to "mind the store"; (2) students are out of school and have more time on their hands; and (3) lonely counterculture hackers increase their attacks.

Control procedures fall into the following categories:

1. Proper authorization of transactions and activities
2. Segregation of duties
3. Project development and acquisition controls
4. Change management controls
5. Design and use of documents and records
6. Safeguarding assets, records, and data
7. Independent checks on performance

Focus 7-1 discusses how a regular audit at an Egyptian firm uncovered inherent problems with their central EBS suite.

Proper Authorization of Transactions and Activities

Because management lacks the time and resources to supervise each company activity and decision, it establishes policies for employees to follow and then empowers them. This empowerment, called ***authorization***, is an important control procedure. Authorizations are often documented by signing, initializing, or entering an authorization code on a document or

FOCUS 7-1 The Rawash Group

The Rawash Group is a joint-stock Egyptian firm engaged in manufacturing and selling passenger cars and commercial vehicles. The firm used the Baan ERP system from 1997 until January 2004, when it was replaced by the Oracle EBS suite.

The firm, by law, is required to undergo a yearly audit. In auditing Oracle's financial modules, the auditors reviewed the IT controls. The key drivers were the sensitivity of information traveling across the group's data network and the significant reliance on the infrastructure supporting the daily sales transactions, order entry operations, and the like. The review also focused on the effectiveness of the information systems and the technology control environment serving the financial transaction and reporting process. Authority limits, periodic changes of log-in credentials, and other controls were missing or not included on the Oracle server.

The audit findings covered the General Ledger, Order Management, Accounts Payable and Receivables, and Inventory modules. The audit examined access to and control of the Oracle application. Segregation of duties and system administration were among the most significant issues identified in the report. The report highlighted the excessive access privileges granted to users over the reviewed modules. Business units' set-up functions—such as creating warehouses, defining units of measures, defining bill of material status, and defining template items—were not appropriately segregated. For example, users were allowed access to business functions that should have been segregated, such as issuance of materials and inventory costing. Similar inconsistencies were identified in other modules. The report advised that the group take corrective actions to rectify these problems: (1) reviewing users' responsibilities, (2) embedding an authorization matrix within the system, (3) developing and implementing access policies and procedures, and (4) regularly updating the responsibilities when changes occur in the firm's organization and ensuing authorizations.

record. Computer systems can record a ***digital signature***, a means of signing a document with data that cannot be forged. Digital signatures are discussed in Chapter 9.

Employees who process transactions should verify the presence of appropriate authorizations. Auditors review transactions to verify proper authorization, as their absence indicates a possible control problem. For example, Jason Scott discovered that some purchases did not have a purchase requisition. Instead, they had been "personally authorized" by Bill Springer, the purchasing vice president. Jason also found that some payments had been authorized without proper supporting documents, such as purchase orders and receiving reports. These findings raise questions about the adequacy of Springer's internal control procedures.

Certain activities or transactions may be of such consequence that management grants ***specific authorization*** for them to occur. For example, management review and approval may be required for sales in excess of $50,000. In contrast, management can authorize employees to handle routine transactions without special approval, a procedure known as ***general authorization***. Management should have written policies on both specific and general authorization for all types of transactions.

Segregation of Duties

Good internal control requires that no single employee be given too much responsibility over business transactions or processes. An employee should not be in a position to commit *and* conceal fraud. Segregation of duties is discussed in two separate sections: segregation of accounting duties and segregation of systems duties.

SEGREGATION OF ACCOUNTING DUTIES As shown in Figure 7-3, effective ***segregation of accounting duties*** is achieved when the following functions are separated:

- *Authorization*—approving transactions and decisions
- *Recording*—preparing source documents; entering data into online systems; maintaining journals, ledgers, files or databases; and preparing reconciliations and performance reports
- *Custody*—handling cash, tools, inventory, or fixed assets; receiving incoming customer checks; writing checks

If one person performs two of these functions, problems can arise. For example, the city treasurer of Fairfax, Virginia, embezzled $600,000. When residents used cash to pay their taxes, she kept the currency and entered the payments on property tax records, but did not report them

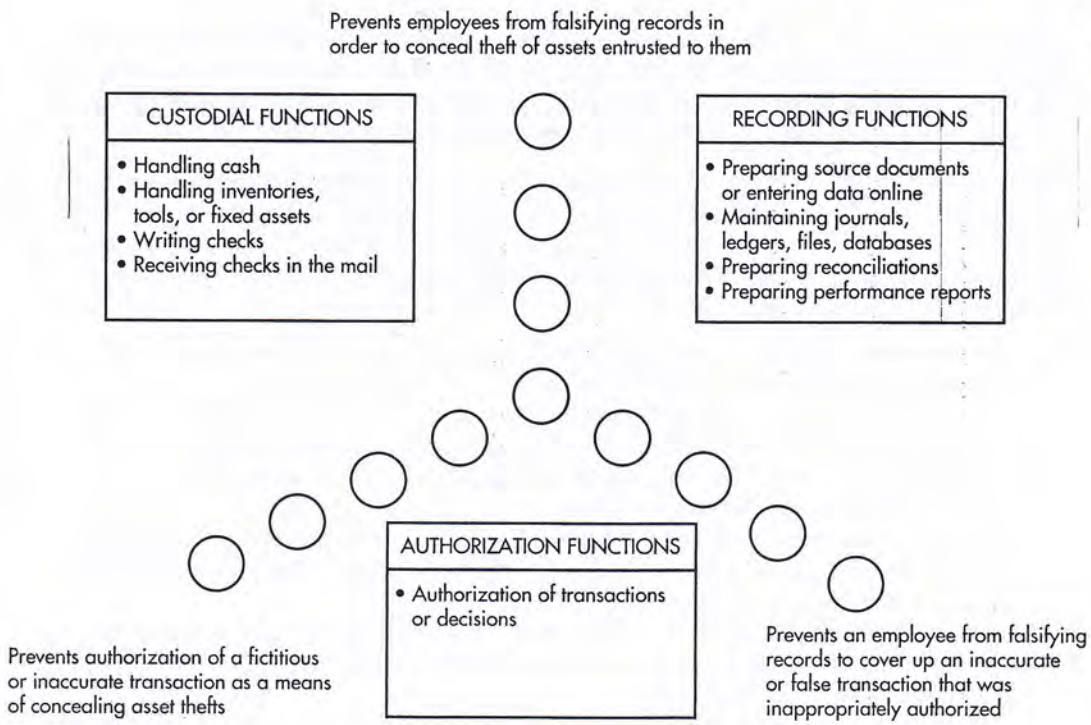


FIGURE 7-3
Separation of Duties

to the controller. Periodically, she made an adjusting journal entry to bring her records into agreement with those of the controller. When she received checks in the mail that would not be missed if not recorded, she put them in the cash register and stole that amount of cash. Because the treasurer was responsible for both the *custody* of cash receipts and the *recording* of those receipts, she was able to steal cash receipts and falsify the accounts to conceal the theft.

In another example, the utilities director of Newport Beach, California, embezzled $1.2 million. Responsible for authorizing transactions, he forged invoices or easement documents authorizing payments to real or fictitious property owners. Finance department officials gave him the checks to deliver to the property owners. He forged signatures and deposited the checks in his own account. Because he was given *custody* of the checks he authorized, he could *authorize* fictitious transactions and steal the payments.

The payroll director of the Los Angeles Dodgers embezzled $330,000. He credited employees for hours not worked and received a kickback of 50% of the extra compensation. He added fictitious names to the Dodgers payroll and cashed the paychecks. The fraud was discovered while he was ill and another employee performed his duties. Because the perpetrator was responsible for *authorizing* the hiring of employees and for *recording* employee hours, he did not need to prepare or handle the paychecks. The company mailed the checks to the address he specified.

Computers can be programmed to perform one or more of the authorization, custody, and recording functions. Segregation of duties is maintained, except that the computer performs the function. For example, people can pay for gas using a credit or debit card. The computer performs both the custody and the recording function. In addition to better internal control, this better serves the customer by increasing convenience and eliminating lines to pay for the gas.

In a system with effective separation of duties, it is difficult for any single employee to embezzle successfully. Detecting fraud where two or more people are in **collusion** to override controls is more difficult because it is much easier to commit and conceal the fraud. For example, two women at a credit card company colluded. One woman authorized new credit card accounts, and the other wrote off unpaid accounts of less than $1,000. The first woman created a new account for each of them using fictitious data. When the amounts outstanding neared the $1,000 limit, the woman in collections wrote them off. The process would then be repeated. They were caught when a jilted boyfriend seeking revenge reported the scheme to the credit card company.

Employees can collude with other employees, customers, or vendors. The most frequent employee/vendor collusion includes billing at inflated prices, performing substandard work and

receiving full payment, payment for nonperformance, duplicate billings, and improperly purchasing more goods from a colluding company. The most frequent employee/customer collusion includes unauthorized loans or insurance payments, receipt of assets or services at unauthorized discount prices, forgiveness of amounts owed, and unauthorized extension of due dates.

SEGREGATION OF SYSTEMS DUTIES In an information system, procedures once performed by separate individuals are combined. Therefore, any person who has unrestricted access to the computer, its programs, and live data could perpetrate and conceal fraud. To combat this threat, organizations implement ***segregation of systems duties***. Authority and responsibility should be divided clearly among the following functions:

1. *Systems administration.* ***Systems administrators*** make sure all information system components operate smoothly and efficiently.
2. *Network management.* ***Network managers*** ensure that devices are linked to the organization's internal and external networks and that those networks operate properly.
3. *Security management.* ***Security management*** makes sure that systems are secure and protected from internal and external threats.
4. *Change management.* ***Change management*** is the process of making sure that changes are made smoothly and efficiently and that they do not negatively affect systems reliability, security, confidentiality, integrity, and availability.
5. *Users.* Users record transactions, authorize data to be processed, and use system output.
6. *Systems analysis.* ***Systems analysts*** help users determine their information needs and design systems to meet those needs.
7. *Programming.* ***Programmers*** take the analysts' design and create a system by writing the computer programs.
8. *Computer operations.* ***Computer operators*** run the software on the company's computers. They ensure that data are input properly, that they are processed correctly, and that output is produced when needed.
9. *Information system library.* The information system librarian maintains custody of corporate databases, files, and programs in a separate storage area called the ***information system library***.
10. *Data control.* The ***data control group*** ensures that source data have been properly approved, monitors the flow of work through the computer, reconciles input and output, maintains a record of input errors to ensure their correction and resubmission, and distributes systems output.

Allowing a person to do two or more of these jobs exposes the company to fraud. For example, if a credit union programmer uses actual data to test her program, she could erase her car loan balance during the test. Likewise, if a computer operator has access to programming logic and documentation, he might be able to increase his salary while processing payroll.

Project Development and Acquisition Controls

It is important to have a proven methodology to govern the development, acquisition, implementation, and maintenance of information systems. It should contain appropriate controls for management approval, user involvement, analysis, design, testing, implementation, and conversion. These methodologies are discussed in Chapters 20 through 22.

Important systems development controls include the following:

1. A ***steering committee*** guides and oversees systems development and acquisition.
2. A ***strategic master plan*** is developed and updated yearly to align an organization's information system with its business strategies. It shows the projects that must be completed, and it addresses the company's hardware, software, personnel, and infrastructure requirements.
3. A ***project development plan*** shows the tasks to be performed, who will perform them, project costs, completion dates, and ***project milestones***—significant points when progress is reviewed and actual and estimated completion times are compared. Each project is assigned to a manager and team who are responsible for its success or failure.
4. A ***data processing schedule*** shows when each task should be performed.

5. *System performance measurements* are established to evaluate the system. Common measurements include ***throughput*** (output per unit of time), ***utilization*** (percentage of time the system is used), and ***response time*** (how long it takes the system to respond).
6. A ***post-implementation review*** is performed after a development project is completed to determine whether the anticipated benefits were achieved.

Some companies hire a ***systems integrator*** to manage a systems development effort involving its own personnel, its client, and other vendors. These development projects are subject to the same cost overruns and missed deadlines as systems developed internally. For example, Westpac Banking began a five-year, $85 million systems development project to decentralize its systems, create new financial products, and downsize its systems department. Three years and $150 million later, no usable results had been attained, and it was clear the scheduled completion date would not be met. With a runaway on its hands, Westpac fired IBM, the primary software developer, and brought in Accenture to review the project and develop recommendations for salvaging it.

Companies using systems integrators should use the same project management processes and controls as internal projects. In addition, they should:

- *Develop clear specifications.* This includes exact descriptions and system definitions, explicit deadlines, and precise acceptance criteria. Suffolk County, New York, spent 12 months and $500,000 preparing detailed specifications for a $16 million criminal justice system before accepting bids. Only 6 of 22 invited integrators bid on the project because of the county's rigorous cost and quality standards. County officials believe their diligent up-front efforts helped ensure their new system's success and saved the county $3 million.
- *Monitor the project.* Companies should establish formal procedures for measuring and reporting a project's status. The best approach is to divide the project into manageable tasks, assign responsibility for each task, and meet at least monthly to review progress and assess quality.

Change Management Controls

Organizations modify existing systems to reflect new business practices and to take advantage of IT advancements. Those in charge of changes should make sure they do not introduce errors and facilitate fraud. Change management controls are discussed in Chapter 10.

Design and Use of Documents and Records

The proper design and use of electronic and paper documents and records help ensure the accurate and complete recording of all relevant transaction data. Their form and content should be as simple as possible, minimize errors, and facilitate review and verification. Documents that initiate a transaction should contain a space for authorizations. Those that transfer assets need a space for the receiving party's signature. Documents should be sequentially prenumbered so each can be accounted for. An audit trail facilitates tracing individual transactions through the system, correcting errors, and verifying system output. Document, form, and input screen design are discussed in Chapter 22.

Safeguard Assets, Records, and Data

A company must protect its cash and physical assets as well as its information. A reporter for Reuters noticed that Intentia, a Swedish software developer, released its first- and second-quarter earnings reports on Web sites with nearly identical Web addresses. He guessed the third-quarter Web address, found their unreleased numbers, and ran a story on the disappointing results. Intentia filed criminal hacking charges, but they were dismissed. The Swedish Stock Exchange censored Intentia for not protecting its financial information.

Employees are a much greater security risk than outsiders are. They are better able to hide their illegal acts, because they know system weakness better. Almost 50% of companies report that insiders access data without the proper authorization. A software engineer at America Online was charged with selling 92 million e-mail addresses he illegally obtained using another employee's ID and password. An Internet gambling business bought the names and used them to increase company earnings by $10,000 to $20,000 a day. The data theft was not uncovered for a year, until an anonymous tipster informed authorities that the gambling business was reselling the names to spammers selling herbal male enhancement products.

Employees also cause unintentional threats, such as accidentally deleting company data, opening virus-laden e-mail attachments, or trying to fix hardware or software without the appropriate expertise. These can result in crashed networks, corrupt data, and hardware and software malfunctions.

Chapters 8 through 10 discuss computer-based controls that help safeguard assets. In addition, it is important to:

- *Create and enforce appropriate policies and procedures.* All too often, policies and procedures are created but not enforced. A laptop with the names, Social Security numbers, and birthdates of 26.5 million people was stolen from the home of a Veteran Affairs (VA) Department analyst. The VA did not enforce its policies that sensitive data be encrypted and not leave VA offices. The cost to taxpayers of notifying all 26.5 million people and buying them a credit-checking service was $100 million. Two years prior to the theft, an inspector general report identified the inadequate control of sensitive data as a weakness, but it had never been addressed.
- *Maintain accurate records of all assets.* Periodically reconcile the recorded amounts of company assets to physical counts of those assets.
- *Restrict access to assets.* Restricting access to storage areas protects inventories and equipment. Cash registers, safes, lockboxes, and safety deposit boxes limit access to cash and paper assets. Over $1 million was embezzled from Perini Corp. because blank checks were kept in an unlocked storeroom. An employee made out checks to fictitious vendors, ran them through an unlocked check-signing machine, and cashed the checks.
- *Protect records and documents.* Fireproof storage areas, locked filing cabinets, backup files, and off-site storage protect records and documents. Access to blank checks and documents should be limited to authorized personnel. In Inglewood, California, a janitor stole 34 blank checks, wrote checks from $50,000 to $470,000, forged the names of city officials, and cashed them.

Independent Checks on Performance

Independent checks on performance, done by someone other than the person who performs the original operation, help ensure that transactions are processed accurately. They include the following:

- *Top-level reviews.* Management should monitor company results and periodically compare actual company performance to (a) planned performance, as shown in budgets, targets, and forecasts; (b) prior period performance; and (c) competitors' performance.
- *Analytical reviews.* An *analytical review* is an examination of the relationships between different sets of data. For example, as credit sales increase, so should accounts receivable. In addition, there are relationships between sales and accounts such as cost of goods sold, inventory, and freight out.
- *Reconciliation of independently maintained records.* Records should be reconciled to documents or records with the same balance. For example, a bank reconciliation verifies that company checking account balances agree with bank statement balances. Another example is comparing subsidiary ledger totals with general ledger totals.
- *Comparison of actual quantities with recorded amounts.* Significant assets are periodically counted and reconciled to company records. At the end of each clerk's shift, cash in a cash register drawer should match the amount on the cash register tape. Inventory should be periodically counted and reconciled to inventory records.
- *Double-entry accounting.* The maxim that debits equal credits provides numerous opportunities for independent checks. Debits in a payroll entry may be allocated to numerous inventory and/or expense accounts; credits are allocated to liability accounts for wages payable, taxes withheld, employee insurance, and union dues. After the payroll entries, comparing total debits and credits is a powerful check on the accuracy of both processes. Any discrepancy indicates the presence of an error.
- *Independent review.* After a transaction is processed, a second person reviews the work of the first, checking for proper authorization, reviewing supporting documents, and checking the accuracy of prices, quantities, and extensions.

Information and Communication

Information and communication constitute the seventh component of the ERM model. This relates directly to the primary purpose of an AIS, which is to gather, record, process, store, summarize, and communicate information about an organization. This includes understanding how transactions are initiated, data are captured, files are accessed and updated, data are processed, and information is reported. It includes understanding accounting records and procedures, supporting documents, and financial statements. These items provide an ***audit trail***, which allows transactions to be traced back and forth between their origination and the financial statements.

According to the AICPA, an AIS has five primary objectives: to identify and record all valid transactions, properly classify transactions, record transactions at their proper monetary value, record transactions in the proper accounting period, and properly present transactions and related disclosures in the financial statements.

Accounting systems generally consist of several subsystems, each designed to process a particular type of transaction using the same sequence of procedures, called accounting cycles. The major accounting cycles and their related control objectives and procedures are detailed in Chapters 12 through 17.

Monitoring

ERM processes must be continuously monitored and modified as needed, and deficiencies must be reported to management. Key methods of monitoring performance include the following:

Perform ERM Evaluations

ERM effectiveness is measured using a formal or a self-assessment ERM evaluation. A team can be formed to conduct the evaluation, or it can be done by internal auditing.

Implement Effective Supervision

Effective supervision involves training and assisting employees, monitoring their performance, correcting errors, and overseeing employees who have access to assets. Supervision is especially important in organizations without responsibility reporting or an adequate segregation of duties.

Use Responsibility Accounting Systems

Responsibility accounting systems include budgets, quotas, schedules, standard costs, and quality standards; reports comparing actual and planned performance; and procedures for investigating and correcting significant variances.

Monitor System Activities

Risk analysis and management software packages review computer and network security measures, detect illegal access, test for weaknesses and vulnerabilities, report weaknesses found, and suggest improvements. Cost parameters can be entered to balance acceptable levels of risk tolerance and cost-effectiveness. Software also monitors and combats viruses, spyware, adware, spam, phishing, and inappropriate e-mails. It blocks pop-up ads, prevents browsers from being hijacked, and validates a phone caller's identity by comparing the caller's voice to a previously recorded voiceprint. Software can help companies recover from malicious actions. One package helped a company recover from a disgruntled employee's rampage. After a negative performance evaluation, the perpetrator ripped cables out of PCs, changed the inventory control files, and edited the password file to stop people from logging on to the network. The software quickly identified the corrupted files and alerted company headquarters. The damage was undone by utility software, which restored the corrupted file to its original status.

All system transactions and activities should be recorded in a log that indicates who accessed what data, when, and from which online device. These logs should be reviewed frequently and used to monitor system activity, trace problems to their source, evaluate employee

productivity, control company costs, fight espionage and hacking attacks, and comply with legal requirements. One company used these logs to analyze why an employee had almost zero productivity and found that he spent six hours a day visiting Internet pornography sites.

The Privacy Foundation estimated that one-third of all American workers with computers are monitored, and that number is expected to increase. Companies who monitor system activities should not violate employee privacy. One way to do that is to have employees agree in writing to written policies that include the following:

- The technology an employee uses on the job belongs to the company.
- E-mails received on company computers are not private and can be read by supervisory personnel. This policy allowed a large pharmaceutical company to identify and terminate an employee who was e-mailing confidential drug-manufacturing data to an external party.
- Employees should not use technology to contribute to a hostile work environment.

Track Purchased Software and Mobile Devices

The Business Software Alliance (BSA) tracks down and fines companies that violate software license agreements. To comply with copyrights and protect themselves from software piracy lawsuits, companies should periodically conduct software audits. There should be enough licenses for all users, and the company should not pay for more licenses than needed. Employees should be informed of the consequences of using unlicensed software.

The increasing number of mobile devices should be tracked and monitored, because their loss could represent a substantial exposure. Items to track are the devices, who has them, what tasks they perform, the security features installed, and what software the company needs to maintain adequate system and network security.

Conduct Periodic Audits

External, internal, and network security audits can assess and monitor risk as well as detect fraud and errors. Informing employees of audits helps resolve privacy issues, deters fraud, and reduces errors. Auditors should regularly test system controls and periodically browse system usage files looking for suspicious activities. During the security audit of a health care company, auditors pretending to be computer support staff persuaded 16 of 22 employees to reveal their user IDs and passwords. They also found that employees testing a new system left the company's network exposed to outside attacks. Systems auditing is explained in Chapter 11.

Internal audits assess the reliability and integrity of financial and operating information, evaluate internal control effectiveness, and assess employee compliance with management policies and procedures as well as applicable laws and regulations. The internal audit function should be organizationally independent of accounting and operating functions. Internal audit should report to the audit committee, not the controller or chief financial officer.

One internal auditor noted that a department supervisor took the office staff to lunch in a limousine on her birthday. Wondering whether her salary could support her lifestyle, he investigated and found she set up several fictitious vendors, sent the company invoices from these vendors, and cashed the checks mailed to her. Over a period of several years, she embezzled over $12 million.

Employ a Computer Security Officer and a Chief Compliance Officer

A *computer security officer (CSO)* is in charge of system security, independent of the information system function, and reports to the chief operating officer (COO) or the CEO. The overwhelming tasks related to SOX and other forms of compliance have led many companies to delegate all compliance issues to a *chief compliance officer (CCO)*. Many companies use outside computer consultants or in-house teams to test and evaluate security procedures and computer systems.

Engage Forensic Specialists

Forensic investigators who specialize in fraud are a fast-growing group in the accounting profession. Their increasing presence is due to several factors, most notably SOX, new accounting rules, and demands by boards of directors that forensic investigations be an ongoing part of the financial reporting and corporate governance process. Most forensic investigators received specialized

training with the FBI, IRS, or other law enforcement agencies. Investigators with the computer skills to ferret out fraud perpetrators are in great demand. The Association of Certified Fraud Examiners sponsors a Certified Fraud Examiner (CFE) professional certification program. To become a CFE, candidates must pass a two-day exam. Currently there are about 30,000 CFEs worldwide.

Computer forensics specialists discover, extract, safeguard, and document computer evidence such that its authenticity, accuracy, and integrity will not succumb to legal challenges. Computer forensics can be compared to performing an "autopsy" on a computer system to determine whether a crime was committed as well as who committed it, and then marshalling the evidence lawyers need to prove the charges in court. Some of the more common matters investigated are improper Internet usage; fraud; sabotage; the loss, theft, or corruption of data; retrieving "erased" information from e-mails and databases; and figuring out who performed certain computer activities. A Deloitte & Touche forensics team uncovered evidence that helped convict a Giant Supermarket purchasing manager who had accepted over $600,000 in supplier kickbacks.

Install Fraud Detection Software

Fraudsters follow distinct patterns and leave clues behind that can be discovered by fraud detection software. ReliaStar Financial used software from IBM to detect the following:

- A Los Angeles chiropractor submitted hundreds of thousands of dollars in fraudulent claims. The software identified an unusual number of patients who lived more than 50 miles away from the doctor's office and flagged these bills for investigation.
- A Long Island doctor submitted weekly bills for a rare and expensive procedure normally done only once or twice in a lifetime.
- A podiatrist saw four patients and billed for 500 separate procedures.

Neural networks (programs with learning capabilities) can accurately identify fraud. The Visa and MasterCard operation at Mellon Bank uses a neural network to track 1.2 million accounts. It can spot illegal credit card use and notify the owner shortly after the card is stolen. It can also spot trends before bank investigators do. For example, an investigator learned about a new fraud from another bank. When he went to check for the fraud, the neural network had already identified it and had printed out transactions that fit its pattern. The software cost the bank less than $1 million and paid for itself in six months.

Implement a Fraud Hotline

People witnessing fraudulent behavior are often torn between two conflicting feelings. Although they want to protect company assets and report fraud perpetrators, they are uncomfortable blowing the whistle, so all too often they remain silent. This reluctance is stronger if they are aware of whistle-blowers who have been ostracized, been persecuted, or suffered damage to their careers.

SOX mandates a mechanism for employees to report fraud and abuse. A ***fraud hotline*** is an effective way to comply with the law and resolve whistle-blower conflict. In one study, researchers found that 33% of 212 frauds were detected through anonymous tips. The insurance industry set up a hotline to control $17 billion a year in fraudulent claims. In the first month, more than 2,250 calls were received; 15% resulted in investigative action. The downside of hotlines is that many calls are not worthy of investigation; some are motivated by a desire for revenge, some are vague reports of wrongdoing, and others have no merit.

Summary and Case Conclusion

One week after Jason and Maria filed their audit report, they were summoned to the office of Northwest's director of internal auditing to explain their findings. Shortly thereafter, a fraud investigation team was dispatched to Bozeman to take a closer look at the situation. Six months later, a company newsletter indicated that the Springer family sold its 10% interest in the business and resigned from all management positions. Two Northwest executives were transferred in to replace them. There was no other word on the audit findings.

Two years later, Jason and Maria worked with Frank Ratliff, a member of the high-level audit team. After hours, Frank told them the investigation team examined a large sample of purchasing transactions and all employee timekeeping and payroll records for a 12-month period. The team also took a detailed physical inventory. They discovered that the problems Jason identified—including missing purchase requisitions, purchase orders, and receiving reports, as well as excessive prices—were widespread. These problems occurred in transactions with three large vendors from whom Springer's had purchased several million dollars of inventory. The investigators discussed the unusually high prices with the vendors but did not receive a satisfactory explanation. The county business-licensing bureau revealed that Bill Springer held a majority ownership interest in each of these companies. By authorizing excessive prices to companies he owned, Springer earned a significant share of several hundred thousand dollars of excessive profits, all at the expense of Northwest Industries.

Several Springer employees were paid for more hours than they worked. Inventory was materially overstated; a physical inventory revealed that a significant portion of recorded inventory did not exist and that some items were obsolete. The adjusting journal entry reflecting Springer's real inventory wiped out much of their profits over the past three years.

When confronted, the Springers vehemently denied breaking any laws. Northwest considered going to the authorities but was concerned that the case was not strong enough to prove in court. Northwest also worried that adverse publicity might damage the company's position in Bozeman. After months of negotiation, the Springers agreed to the settlement reported in the newsletter. Part of the settlement was that no public statement would be made about any alleged fraud or embezzlement involving the Springers. According to Frank, this policy was normal. In many fraud cases, settlements are reached quietly, with no legal action taken, so that the company can avoid adverse publicity.

Key Terms

threat 204
exposure 204
impact 204
likelihood 204
internal control 204
preventive control 205
detective control 205
corrective control 205
general control 205
application control 205
belief system 205
boundary system 205
diagnostic control system 205
interactive control system 205
Foreign Corrupt Practices Act 205
Sarbanes–Oxley Act (SOX) 205
Public Company Accounting Oversight Board (PCAOB) 206
Control Objectives for Information and Related Technology (COBIT) 206
Committee of Sponsoring Organizations (COSO) 207
Internal Control—Integrated Framework (IC) 207
Enterprise Risk Management—Integrated Framework (ERM) 207
internal environment 208
risk appetite 209
audit committee 209
policy and procedures manual 210
background check 210
strategic objective 212
operations objective 212
reporting objective 212
compliance objective 212
event 212
inherent risk 213
residual risk 213
expected loss 214
control activities 215
authorization 215
digital signature 216
specific authorization 216
general authorization 216
segregation of accounting duties 216
collusion 217
segregation of systems duties 218
systems administrator 218
network manager 218
security management 218
change management 218
systems analyst 218
programmer 218
computer operator 218
information system library 218
data control group 218
steering committee 218
strategic master plan 218
project development plan 218
project milestone 218
data processing schedule 218
system performance measurements 219
throughput 219
utilization 219

response time 219
post-implementation review 219
systems integrator 219
analytical review 220
audit trail 221
computer security officer (CSO) 222
chief compliance officer (CCO) 222
forensic investigators 222
computer forensics specialist 223
neural network 223
fraud hot line 223

AIS IN ACTION

Chapter Quiz

1. COSO identified five interrelated components of internal control. Which of the following is NOT one of those five?
   a. risk assessment
   b. internal control policies
   c. monitoring
   d. information and communication

2. In the ERM model, COSO specified four types of objectives that management must meet to achieve company goals. Which of the following is NOT one of those types?
   a. responsibility objectives
   b. strategic objectives
   c. compliance objectives
   d. reporting objectives
   e. operations objectives

3. Which of the following statements is true?
   a. COSO's enterprise risk management framework is narrow in scope and is limited to financial controls.
   b. COSO's internal control integrated framework has been widely accepted as the authority on internal controls.
   c. The Foreign Corrupt Practices Act had no impact on internal accounting control systems.
   d. It is easier to add controls to an already designed system than to include them during the initial design stage.

4. All other things being equal, which of the following is true?
   a. Detective controls are superior to preventive controls.
   b. Corrective controls are superior to preventive controls.
   c. Preventive controls are equivalent to detective controls.
   d. Preventive controls are superior to detective controls.

5. Which of the following statements about the control environment is FALSE?
   a. Management's attitudes toward internal control and ethical behavior have little impact on employee beliefs or actions.
   b. An overly complex or unclear organizational structure may be indicative of problems that are more serious.
   c. A written policy and procedures manual is an important tool for assigning authority and responsibility.
   d. Supervision is especially important in organizations that cannot afford elaborate responsibility reporting or are too small to have an adequate separation of duties.

6. To achieve effective segregation of duties, certain functions must be separated. Which of the following is the correct listing of the accounting-related functions that must be segregated?
   a. control, recording, and monitoring
   b. authorization, recording, and custody
   c. control, custody, and authorization
   d. monitoring, recording, and planning

7. Which of the following is NOT an independent check?
   a. bank reconciliation
   b. periodic comparison of subsidiary ledger totals to control accounts
   c. trial balance
   d. re-adding the total of a batch of invoices and comparing it with your first total

8. Which of the following is a control procedure relating to both the design and use of documents and records?
   a. locking blank checks in a drawer
   b. reconciling the bank account
   c. sequentially prenumbering sales invoices
   d. comparing actual physical quantities with recorded amounts

9. Which of the following is the correct order of the risk assessment steps discussed in this chapter?
   a. Identify threats, estimate risk and exposure, identify controls, and estimate costs and benefits.
   b. Identify controls, estimate risk and exposure, identify threats, and estimate costs and benefits.
   c. Estimate risk and exposure, identify controls, identify threats, and estimate costs and benefits.
   d. Estimate costs and benefits, identify threats, identify controls, and estimate risk and exposure.

10. Your current system is deemed to be 90% reliable. A major threat has been identified with an impact of $3,000,000. Two control procedures exist to deal with the threat. Implementation of control A would cost $100,000 and reduce the likelihood to 6%. Implementation of control B would cost $140,000 and reduce the likelihood to 4%. Implementation of both controls would cost $220,000 and reduce the likelihood to 2%. Given the data, and based solely on an economic analysis of costs and benefits, what should you do?
    a. Implement control A only.
    b. Implement control B only.
    c. Implement both controls A and B.
    d. Implement neither control.

Discussion Questions

7.1. Answer the following questions about the audit of Springer's Lumber & Supply.
   a. What deficiencies existed in the internal environment at Springer's?
   b. Do you agree with the decision to settle with the Springers rather than to prosecute them for fraud and embezzlement? Why or why not?
   c. Should the company have told Jason and Maria the results of the high-level audit? Why or why not?

7.2. Effective segregation of duties is sometimes not economically feasible in a small business. What internal control elements do you think can help compensate for this threat?

7.3. One function of the AIS is to provide adequate controls to ensure the safety of organizational assets, including data. However, many people view control procedures as "red tape." They also believe that instead of producing tangible benefits, business controls create resentment and loss of company morale. Discuss this position.

7.4. In recent years, Supersmurf's external auditors have given clean opinions on its financial statements and favorable evaluations of its internal control systems. Discuss whether it is necessary for this corporation to take any further action to comply with the Sarbanes–Oxley Act.

7.5. When you go to a movie theater, you buy a prenumbered ticket from the cashier. This ticket is handed to another person at the entrance to the movie. What kinds of irregularities is the theater trying to prevent? What controls is it using to prevent these irregularities? What remaining risks or exposures can you identify?

7.6. Some restaurants use customer checks with prenumbered sequence codes. Each food server uses these checks to write up customer orders. Food servers are told not to destroy any customer checks; if a mistake is made, they are to void that check and write a new one. All voided checks are to be turned in to the manager daily. How does this policy help the restaurant control cash receipts?

7.7. Compare and contrast the following three frameworks: COBIT, COSO Integrated Control, and ERM.

7.8. Explain what an event is. Using the Internet as a resource, create a list of some of the many internal and external factors that COSO indicated could influence events and affect a company's ability to implement its strategy and achieve its objectives.

7.9. Explain what is meant by objective setting, and describe the four types of objectives used in ERM.

7.10. Discuss several ways that ERM processes can be continuously monitored and modified so that deficiencies are reported to management.

Problems

7.1. You are an audit supervisor assigned to a new client, Go-Go Corporation, which is listed on the New York Stock Exchange. You visited Go-Go's corporate headquarters to become acquainted with key personnel and to conduct a preliminary review of the company's accounting policies, controls, and systems. During this visit, the following events occurred:

a. You met with Go-Go's audit committee, which consists of the corporate controller, treasurer, financial vice president, and budget director.
b. You recognized the treasurer as a former aide to Ernie Eggers, who was convicted of fraud several years ago.
c. Management explained its plans to change accounting methods for depreciation from the accelerated to the straight-line method. Management implied that if your firm does not concur with this change, Go-Go will employ other auditors.
d. You learned that the financial vice president manages a staff of five internal auditors.
e. You noted that all management authority seems to reside with three brothers, who serve as chief executive officer, president, and financial vice president.
f. You were told that the performance of division and department managers is evaluated on a subjective basis, because Go-Go's management believes that formal performance evaluation procedures are counterproductive.
g. You learned that the company has reported increases in earnings per share for each of the past 25 quarters; however, earnings during the current quarter have leveled off and may decline.
h. You reviewed the company's policy and procedures manual, which listed policies for dealing with customers, vendors, and employees.
i. Your preliminary assessment is that the accounting systems are well designed and that they employ effective internal control procedures.
j. Some employees complained that some managers occasionally contradict the instructions of other managers regarding proper data security procedures.
k. After a careful review of the budget for data security enhancement projects, you feel the budget appears to be adequate.
l. The enhanced network firewall project appeared to be on a very aggressive implementation schedule. The IT manager mentioned that even if he put all of his personnel on the project for the next five weeks, he still would not complete the project in time. The

manager has mentioned this to company management, which seems unwilling to modify the schedule.

m. Several new employees have had trouble completing some of their duties, and they do not appear to know who to ask for help.

n. Go-Go's strategy is to achieve consistent growth for its shareholders. However, its policy is not to invest in any project unless its payback period is no more than 48 months and yields an internal rate of return that exceeds its cost of capital by 3%.

o. You observe that company purchasing agents wear clothing and exhibit other paraphernalia from major vendors. The purchasing department manager proudly displays a picture of himself holding a big fish on the deck of a luxury fishing boat that has the logo of a major Go-Go vendor painted on its wheelhouse.

Required

The information you have obtained suggests potential problems relating to Go-Go's internal environment. Identify the problems, and explain them in relation to the internal environment concepts discussed in this chapter.

7.2. Explain how the principle of separation of duties is violated in each of the following situations. Also, suggest one or more procedures to reduce the risk and exposure highlighted in each example.

a. A payroll clerk recorded a 40-hour workweek for an employee who had quit the previous week. He then prepared a paycheck for this employee, forged her signature, and cashed the check.

b. While opening the mail, a cashier set aside, and subsequently cashed, two checks payable to the company on account.

c. A cashier prepared a fictitious invoice from a company using his brother-in-law's name. He wrote a check in payment of the invoice, which the brother-in-law later cashed.

d. An employee of the finishing department walked off with several parts from the storeroom and recorded the items in the inventory ledger as having been issued to the assembly department.

e. A cashier cashed a check from a customer in payment of an account receivable, pocketed the cash, and concealed the theft by properly posting the receipt to the customer's account in the accounts receivable ledger.

f. Several customers returned clothing purchases. Instead of putting the clothes into a return bin to be put back on the rack, a clerk put the clothing in a separate bin under some cleaning rags. After her shift, she transferred the clothes to a gym bag and took them home.

g. A receiving clerk noticed that four cases of MP3 players were included in a shipment when only three were ordered. The clerk put the extra case aside and took it home after his shift ended.

h. An insurance claims adjuster had check-signing authority of up to $6,000. The adjuster created three businesses that billed the insurance company for work not performed on valid claims. The adjuster wrote and signed checks to pay for the invoices, none of which exceeded $6,000.

i. An accounts payable clerk recorded invoices received from a company that he and his wife owned and authorized their payment.

j. A cashier created false purchase return vouchers to hide his theft of several thousand dollars from his cash register.

k. A purchasing agent received a 10% kickback of the invoice amount for all purchases made from a specific vendor.

7.3. The following description represents the policies and procedures for agent expense reimbursements at Excel Insurance Company.

Agents submit a completed expense reimbursement form to their branch manager at the end of each week. The branch manager reviews the expense report to determine whether the claimed expenses are reimbursable based on the company's expense reimbursement policy and reasonableness of amount. The company's policy

manual states that agents are to document any questionable expense item and that the branch manager must approve in advance expenditures exceeding $500.

After the expenses are approved, the branch manager sends the expense report to the home office. There, accounting records the transaction, and cash disbursements prepares the expense reimbursement check. Cash disbursements sends the expense reimbursement checks to the branch manager, who distributes them to the agents.

To receive cash advances for anticipated expenses, agents must complete a Cash Advance Approval form. The branch manager reviews and approves the Cash Advance Approval form and sends a copy to accounting and another to the agent. The agent submits the copy of the Cash Advance Approval form to the branch office cashier to obtain the cash advance.

At the end of each month, internal audit at the home office reconciles the expense reimbursements. It adds the total dollar amounts on the expense reports from each branch, subtracts the sum of the dollar totals on each branch's Cash Advance Approval form, and compares the net amount to the sum of the expense reimbursement checks issued to agents. Internal audit investigates any differences.

Required

Identify the internal control strengths and weaknesses in Excel's expense reimbursement process. Look for authorization, recording, safeguarding, and reconciliation strengths and weaknesses. (*CMA Examination, adapted*)

7.4. The Gardner Company, a client of your firm, has come to you with the following problem. It has three clerical employees who must perform the following functions:

a. Maintain the general ledger
b. Maintain the accounts payable ledger
c. Maintain the accounts receivable ledger
d. Prepare checks for signature
e. Maintain the cash disbursements journal
f. Issue credits on returns and allowances
g. Reconcile the bank account
h. Handle and deposit cash receipts

Assuming equal abilities among the three employees, the company asks you to assign the eight functions to them to maximize internal control. Assume that these employees will perform no accounting functions other than the ones listed.

Required

a. List four possible unsatisfactory pairings of the functions.
b. State how you would distribute the functions among the three employees. Assume that with the exception of the nominal jobs of the bank reconciliation and the issuance of credits on returns and allowances, all functions require an equal amount of time. (*CPA Examination, adapted*)

7.5. During a recent review, ABC Corporation discovered that it has a serious internal control problem. It is estimated that the impact associated with this problem is $1 million and that the likelihood is currently 5%. Two internal control procedures have been proposed to deal with this problem. Procedure A would cost $25,000 and reduce likelihood to 2%; procedure B would cost $30,000 and reduce likelihood to 1%. If both procedures were implemented, likelihood would be reduced to 0.1%.

Required

a. What is the estimated expected loss associated with ABC Corporation's internal control problem before any new internal control procedures are implemented?
b. Compute the revised estimate of expected loss if procedure A were implemented, if procedure B were implemented, and if both procedures were implemented.
c. Compare the estimated costs and benefits of procedure A, procedure B, and both procedures combined. If you consider only the estimates of cost and benefit, which procedure(s) should be implemented?

d. What other factors might be relevant to the decision?
e. Use the Goal Seek function in Microsoft Excel to determine the likelihood of occurrence without the control and the reduction in expected loss if the net benefit/cost is 0. Do this for procedure A, procedure B, and both procedures together.

7.6. The management at Covington, Inc., recognizes that a well-designed internal control system provides many benefits. Among the benefits are reliable financial records that facilitate decision making and a greater probability of preventing or detecting errors and fraud. Covington's internal auditing department periodically reviews the company's accounting records to determine the effectiveness of internal controls. In its latest review, the internal audit staff found the following eight conditions:

1. Daily bank deposits do not always correspond with cash receipts.
2. Bad debt write-offs are prepared and approved by the same employee.
3. There are occasional discrepancies between physical inventory counts and perpetual inventory records.
4. Alterations have been made to physical inventory counts and to perpetual inventory records.
5. There are many customer refunds and credits.
6. Many original documents are missing or lost. However, there are substitute copies of all missing originals.
7. An unexplained decrease in the gross profit percentage has occurred.
8. Many documents are not approved.

Required

For each of the eight conditions detected by the Covington internal audit staff:

a. Describe a possible cause of the condition.
b. Recommend actions to be taken and/or controls to be implemented that would correct the condition. (*CMA, adapted*)

7.7. Consider the following two situations:

1. Many employees of a firm that manufactures small tools pocket some of the tools for their personal use. Because the quantities taken by any one employee are immaterial, the individual employees do not consider the act as fraudulent or detrimental to the company. The company is now large enough to hire an internal auditor. One of the first things she did was to compare the gross profit rates for industrial tools to the gross profit for personal tools. Noting a significant difference, she investigated and uncovered the employee theft.
2. A manufacturing firm's controller created a fake subsidiary. He then ordered goods from the firm's suppliers, told them to ship the goods to a warehouse he rented, and approved the vendor invoices for payment when they arrived. The controller later sold the diverted inventory items, and the proceeds were deposited to the controller's personal bank account. Auditors suspected something was wrong when they could not find any entries regarding this fake subsidiary office in the property, plant, and equipment ledgers or a title or lease for the office in the real-estate records.

Required

For the situations presented, describe the recommendations the internal auditors should make to prevent similar problems in the future. (*CMA, adapted*)

7.8. Tralor Corporation manufactures and sells several different lines of small electric components. Its internal audit department completed an audit of its expenditure processes. Part of the audit involved a review of the internal accounting controls for payables, including the controls over the authorization of transactions, accounting for transactions, and the protection of assets. The auditors noted the following items:

1. Routine purchases are initiated by inventory control notifying the purchasing department of the need to buy goods. The purchasing department fills out a prenumbered purchase order and gets it approved by the purchasing manager. The original of the five-part purchase order goes to the vendor. The other four copies are for purchasing, the user department, receiving for use as a receiving report, and accounts payable.

2. For efficiency and effectiveness, purchases of specialized goods and services are negotiated directly between the user department and the vendor. Company procedures require that the user department and the purchasing department approve invoices for any specialized goods and services before making payment.
3. Accounts payable maintains a list of employees who have purchase order approval authority. The list was updated two years ago and is seldom used by accounts payable clerks.
4. Prenumbered vendor invoices are recorded in an invoice register that indicates the receipt date, whether it is a special order, when a special order is sent to the requesting department for approval, and when it is returned. A review of the register indicated that there were seven open invoices for special purchases, which had been forwarded to operating departments for approval over 30 days previously and had not yet been returned.
5. Prior to making entries in accounting records, the accounts payable clerk checks the mathematical accuracy of the transaction, makes sure that all transactions are properly documented (the purchase order matches the signed receiving report and the vendor's invoice), and obtains departmental approval for special purchase invoices.
6. All approved invoices are filed alphabetically. Invoices are paid on the 5th and 20th of each month, and all cash discounts are taken regardless of the terms.
7. The treasurer signs the checks and cancels the supporting documents. An original document is required for a payment to be processed.
8. Prenumbered blank checks are kept in a locked safe accessible only to the cash disbursements department. Other documents and records maintained by the accounts payable section are readily accessible to all persons assigned to the section and to others in the accounting function.

Required

Review the eight items listed, and decide whether they represent an internal control strength or weakness.

a. For each internal control strength you identified, explain how the procedure helps achieve good authorization, accounting, or asset protection control.
b. For each internal control weakness you identified, explain why it is a weakness and recommend a way to correct the weakness. (*CMA, adapted*)

7.9. Lancaster Company makes electrical parts for contractors and home improvement retail stores. After their annual audit, Lancaster's auditors commented on the following items regarding internal controls over equipment:

1. The operations department that needs the equipment normally initiates a purchase requisition for equipment. The operations department supervisor discusses the proposed purchase with the plant manager. If there are sufficient funds in the requesting department's equipment budget, a purchase requisition is submitted to the purchasing department once the plant manager is satisfied that the request is reasonable.
2. When the purchasing department receives either an inventory or an equipment purchase requisition, the purchasing agent selects an appropriate supplier and sends them a purchase order.
3. When equipment arrives, the user department installs it. The property, plant, and equipment control accounts are supported by schedules organized by year of acquisition. The schedules are used to record depreciation using standard rates, depreciation methods, and salvage values for each type of fixed asset. These rates, methods, and salvage values were set 10 years ago during the company's initial year of operation.
4. When equipment is retired, the plant manager notifies the accounting department so the appropriate accounting entries can be made.
5. There has been no reconciliation since the company began operations between the accounting records and the equipment on hand.

Required

Identify the internal control weaknesses in Lancaster's system, and recommend ways to correct them. (*CMA, adapted*)

7.10. The Langston Recreational Company (LRC) manufactures ice skates for racing, figure skating, and hockey. The company is located in Kearns, Utah, so it can be close to the Olympic Ice Shield, where many Olympic speed skaters train.

Given the precision required to make skates, tracking manufacturing costs is very important to management so it can price the skates appropriately. To capture and collect manufacturing costs, the company acquired an automated cost accounting system from a national vendor. The vendor provides support, maintenance, and data and program backup service for LRC's system.

LRC operates one shift, five days a week. All manufacturing data are collected and recorded by Saturday evening so that the prior week's production data can be processed. One of management's primary concerns is how the actual manufacturing process costs compare with planned or standard manufacturing process costs. As a result, the cost accounting system produces a report that compares actual costs with standards costs and provides the difference, or variance. Management focuses on significant variances as one means of controlling the manufacturing processes and calculating bonuses.

Occasionally, errors occur in processing a week's production cost data, which requires the entire week's cost data to be reprocessed at a cost of $34,500. The current risk of error without any control procedures is 8%. LRC's management is currently considering a set of cost accounting control procedures that is estimated to reduce the risk of the data errors from 8% to 3%. This data validation control procedure is projected to cost $1,000 per week.

Required

a. Perform a cost/benefit analysis of the data validation control procedures.
b. Based on your analysis, make a recommendation to management regarding the control procedure.
c. The current risk of data errors without any control procedures is estimated to be 8%. The data control validation procedure costs $1,000 and reduces the risk to 3%. At some point between 8% and 3% is a point of indifference—that is, Cost of reprocessing the data without controls = Cost of processing the data with the controls + Cost of controls. Use a spreadsheet application such as Excel Goal Seek to find the solution.

7.11. Spring Water Spa Company is a 15-store chain in the Midwest that sells hot tubs, supplies, and accessories. Each store has a full-time, salaried manager and an assistant manager. The sales personnel are paid an hourly wage and a commission based on sales volume.

The company uses electronic cash registers to record each transaction. The salesperson enters his or her employee number at the beginning of his/her shift. For each sale, the salesperson rings up the order by scanning the item's bar code, which then displays the item's description, unit price, and quantity (each item must be scanned). The cash register automatically assigns a consecutive number to each transaction. The cash register prints a sales receipt that shows the total, any discounts, the sales tax, and the grand total.

The salesperson collects payment from the customer, gives the receipt to the customer, and either directs the customer to the warehouse to obtain the items purchased or makes arrangements with the shipping department for delivery. The salesperson is responsible for using the system to determine whether credit card sales are approved and for approving both credit sales and sales paid by check. Sales returns are handled in exactly the reverse manner, with the salesperson issuing a return slip when necessary.

At the end of each day, the cash registers print a sequentially ordered list of sales receipts and provide totals for cash, credit card, and check sales, as well as cash and credit card returns. The assistant manager reconciles these totals to the cash register tapes, cash in the cash register, the total of the consecutively numbered sales invoices, and the return slips. The assistant manager prepares a daily reconciled report for the store manager's review.

Cash sales, check sales, and credit card sales are reviewed by the manager, who prepares the daily bank deposit. The manager physically makes the deposit at the bank and files the validated deposit slip. At the end of the month, the manager performs the bank reconciliation. The cash register tapes, sales invoices, return slips, and reconciled report are mailed daily to corporate headquarters to be processed with files from all the other stores. Corporate headquarters returns a weekly Sales and Commission Activity Report to each store manager for review.

Required

Please respond to the following questions about Spring Water Spa Company's operations:

a. The fourth component of the COSO ERM framework is risk assessment. What risk(s) does Spring Water face?
b. Identify control strengths in Spring Water's sales/cash receipts system.
c. The sixth component of the COSO ERM framework deals with control activities. What control activities do these strengths fall under?
d. What problems were avoided or risks mitigated by the controls identified in question b?
e. How might Spring Water improve its system of controls?

7.12. PriceRight Electronics (PEI) is a small wholesale discount supplier of electronic instruments and parts. PEI's competitive advantage is its deep-discount, three-day delivery guarantee, which allows retailers to order materials often to minimize in-store inventories. PEI processes its records with stand-alone, incompatible computer systems except for integrated enterprise resource planning (ERP) inventory and accounts receivable modules. PEI decided to finish integrating its operations with more ERP modules, but because of cash flow considerations, this needs to be accomplished on a step-by-step basis.

It was decided that the next function to be integrated should be sales order processing to enhance quick response to customer needs. PEI implemented and modified a commercially available software package to meet PEI's operations. In an effort to reduce the number of slow-paying or delinquent customers, PEI installed Web-based software that links to the Web site of a commercial credit rating agency to check customer credit at the time of purchase. The following are the new sales order processing system modules:

- ***Sales***. Sales orders are received by telephone, fax, e-mail, Web site entry, or standard mail. They are entered into the sales order system by the Sales department. If the order does not cause a customer to exceed his credit limit, the system generates multiple copies of the sales order.
- ***Credit***. When orders are received from new customers, the system automatically accesses the credit rating Web site and suggests an initial credit limit. On a daily basis, the credit manager reviews new customer applications for creditworthiness, reviews the suggested credit limits, and accepts or changes the credit limits in the customer database. On a monthly basis, the credit manager reviews the accounts receivable aging report to identify slow-paying or delinquent accounts for potential revisions to or discontinuance of credit. As needed, the credit manager issues credit memos for merchandise returns based on requests from customers and forwards copies of the credit memos to Accounting for appropriate account receivable handling.
- ***Warehousing***. Warehouse personnel update the inventory master file for inventory purchases and sales, confirm availability of materials to fill sales orders, and establish back orders for sales orders that cannot be completed from stock on hand. Warehouse personnel gather and forward inventory to Shipping and Receiving along with the corresponding sales orders. They also update the inventory master file for merchandise returned to Receiving.
- ***Shipping and receiving***. Shipping and Receiving accepts inventory and sales orders from Warehousing, packs and ships the orders with a copy of the sales order as a packing slip, and forwards a copy of the sales order to Billing. Customer inventory returns are unpacked, sorted, inspected, and sent to Warehousing.
- ***Accounting***. Billing prices all sales orders received, which is done approximately 5 days after the order ships. To spread the work effort throughout the month, customers are placed in one of six 30-day billing cycles. Monthly statements, prepared by Billing, are sent to customers during the cycle billing period. Outstanding carry-forward balances reported by Accounts Receivable and credit memos prepared by the credit manager are included on the monthly statement. Billing also prepares electronic sales and credit memos for each cycle. Electronic copies of invoices and credit memos are forwarded to Accounts Receivable for entry into the accounts receivable master file by customer account. An aging report is prepared at the end of each month and forwarded to the credit manager. The general accounting office staff

access the accounts receivable master file that reflects total charges and credits processed through the accounts receivable system for each cycle. General accounting runs a query to compare this information to the electronic sales and credit memo and posts the changes to the general ledger master file.

Required

a. Identify the internal control strengths in PEI's system.
b. Identify the internal control weaknesses in PEI's system, and suggest ways to correct them.

Case 7-1 The Greater Providence Deposit & Trust Embezzlement

Nino Moscardi, president of Greater Providence Deposit & Trust (GPD&T), received an anonymous note in his mail stating that a bank employee was making bogus loans. Moscardi asked the bank's internal auditors to investigate the transactions detailed in the note. The investigation led to James Guisti, manager of a North Providence branch office and a trusted 14-year employee who had once worked as one of the bank's internal auditors. Guisti was charged with embezzling $1.83 million from the bank using 67 phony loans taken out over a three-year period.

Court documents revealed that the bogus loans were 90-day notes requiring no collateral and ranging in amount from $10,000 to $63,500. Guisti originated the loans; when each one matured, he would take out a new loan, or rewrite the old one, to pay the principal and interest due. Some loans had been rewritten five or six times.

The 67 loans were taken out by Guisti in five names, including his wife's maiden name, his father's name, and the names of two friends. These people denied receiving stolen funds or knowing anything about the embezzlement. The fifth name was James Vanesse, who police said did not exist. The Social Security number on Vanesse's loan application was issued to a female, and the phone number belonged to a North Providence auto dealer.

Lucy Fraioli, a customer service representative who cosigned the checks, said Guisti was her supervisor and she thought nothing was wrong with the checks, though she did not know any of the people. Marcia Perfetto, head teller, told police she cashed checks for Guisti made out to four of the five persons. Asked whether she gave the money to Guisti when he gave her checks to cash, she answered, "Not all of the time," though she could not recall ever having given the money directly to any of the four, whom she did not know.

Guisti was authorized to make consumer loans up to a certain dollar limit without loan committee approvals, which is a standard industry practice. Guisti's original lending limit was $10,000, the amount of his first fraudulent loan. The dollar limit was later increased to $15,000 and then increased again to $25,000. Some of the loans, including the one for $63,500, far exceeded his lending limit. In addition, all loan applications should have been accompanied by the applicant's credit history report, purchased from an independent credit rating firm. The loan taken out in the fictitious name would not have had a credit report and should have been flagged by a loan review clerk at the bank's headquarters.

News reports raised questions about why the fraud was not detected earlier. State regulators and the bank's internal auditors failed to detect the fraud. Several reasons were given for the failure to find the fraud earlier. First, in checking for bad loans, bank auditors do not examine all loans and generally focus on loans much larger than the ones in question. Second, Greater Providence had recently dropped its computer services arrangement with a local bank in favor of an out-of-state bank. This changeover may have reduced the effectiveness of the bank's control procedures. Third, the bank's loan review clerks were rotated frequently, making follow-up on questionable loans more difficult.

Guisti was a frequent gambler and used the embezzled money to pay gambling debts. The bank's losses totaled $624,000, which was less than the $1.83 million in bogus loans, because Guisti used a portion of the borrowed money to repay loans as they came due. The bank's bonding company covered the loss.

The bank experienced other adverse publicity prior to the fraud's discovery. First, the bank was fined $50,000 after pleading guilty to failure to report cash transactions exceeding $10,000, which is a felony. Second, bank owners took the bank private after a lengthy public battle with the State Attorney General, who alleged that the bank inflated its assets and overestimated its capital surplus to make its balance sheet look stronger. The bank denied this charge.

1. How did Guisti commit the fraud, conceal it, and convert the fraudulent actions to personal gain?
2. Good internal controls require that the custody, recording, and authorization functions be separated. Explain which of those functions Guisti had and how the failure to segregate them facilitated the fraud.
3. Identify the preventive, detective, and corrective controls at GPD&T, and discuss whether they were effective.
4. Explain the pressures, opportunities, and rationalizations that were present in the Guisti fraud.

5. Discuss how Greater Providence Deposit & Trust might improve its control procedures over the disbursement of loan funds to minimize the risk of this type of fraud. In what way does this case indicate a lack of proper segregation of duties?
6. Discuss how Greater Providence might improve its loan review procedures at bank headquarters to minimize its fraud risk. Was it a good idea to rotate the assignments of loan review clerks? Why or why not?
7. Discuss whether Greater Providence's auditors should have been able to detect this fraud.
8. Are there any indications that the internal environment at Greater Providence may have been deficient? If so, how could it have contributed to this embezzlement?

Source: John Kostrezewa, "Charge: Embezzlement," *Providence Journal-Bulletin* (July 31, 1988): F-1.

AIS IN ACTION SOLUTIONS

Quiz Key

1. COSO identified five interrelated components of internal control. Which of the following is NOT one of those five?
   a. risk assessment (Incorrect. The organization must be aware of and deal with the risks it faces.)
   ▶ b. internal control policies (Correct. Internal control policies are NOT one of COSO's five components of internal control. However, control environment and control activities are two of the five internal control framework components.)
   c. monitoring (Incorrect. The entire internal control process must be monitored, and modifications made as necessary.)
   d. information and communication (Incorrect. The primary purpose of an AIS is to process and communicate information about an organization, and these activities are an essential part of an internal control system.)

2. In the ERM model, COSO specified four types of objectives that management must meet to achieve company goals. Which of the following is NOT one of those types?
   ▶ a. responsibility objectives (Correct. Responsibility objectives are NOT one of the objectives in COSO's ERM model.)
   b. strategic objectives (Incorrect. Strategic objectives are high-level goals aligned with the company's mission and are one of the objectives in COSO's ERM model.)
   c. compliance objectives (Incorrect. Compliance objectives help the company comply with all applicable laws and regulations and are one of the objectives in COSO's ERM model.)
   d. reporting objectives (Incorrect. Reporting objectives help ensure the accuracy, completeness, and reliability of internal and external reports and are one of the objectives in COSO's ERM model.)
   e. operations objectives (Incorrect. Operations objectives deal with the effectiveness and efficiency of operations and are one of the objectives in COSO's ERM model.)

3. Which of the following statements is true?
   a. COSO's enterprise risk management framework is narrow in scope and is limited to financial controls. (Incorrect. The ERM framework incorporates all kinds of internal controls, not just financial controls, and provides an all-encompassing focus on the broader subject of enterprise risk management.)
   ▶ b. COSO's internal control integrated framework has been widely accepted as the authority on internal controls. (Correct. The internal control integrated framework is the accepted authority on internal controls and is incorporated into policies, rules, and regulations that are used to control business activities.)

c. The Foreign Corrupt Practices Act had no impact on internal accounting control systems. (Incorrect. The Foreign Corrupt Practices Act specifically requires corporations to maintain good systems of internal accounting control.)
d. It is easier to add controls to an already designed system than to include them during the initial design stage. (Incorrect. The opposite is true: It is easier to include internal controls at the initial design stage than after the system is already designed.)

4. All other things being equal, which of the following is true?
a. Detective controls are superior to preventive controls. (Incorrect. The reverse is true—preventive controls are superior to detective controls. Preventive controls keep an error or irregularity from occurring. Detective controls uncover an error or irregularity after the fact.)
b. Corrective controls are superior to preventive controls. (Incorrect. The reverse is true—preventive controls are superior to corrective controls. Preventive controls keep an error or irregularity from occurring. Corrective controls fix an error after the fact.)
c. Preventive controls are equivalent to detective controls. (Incorrect. Preventive controls keep an error or irregularity from occurring. Detective controls uncover an error or irregularity after the fact.)
▶ d. Preventive controls are superior to detective controls. (Correct. With respect to controls, it is always of utmost importance to prevent errors from occurring.)

5. Which of the following statements about the control environment is FALSE?
▶ a. Management's attitudes toward internal control and ethical behavior have little impact on employee beliefs or actions. (Correct. This statement is false. Management's attitude toward internal control is critical to the organization's effectiveness and success. They set the "tone at the top" that other employees follow.)
b. An overly complex or unclear organizational structure may be indicative of problems that are more serious. (Incorrect. This is a true statement. Management may intentionally build overly complex or unclear organizational structures to hide fraud or errors.)
c. A written policy and procedures manual is an important tool for assigning authority and responsibility. (Incorrect. This is a true statement. A written policy and procedures manual explains proper business practices, describes the knowledge and experience needed by key personnel, and lists the resources provided to carry out specific duties.)
d. Supervision is especially important in organizations that cannot afford elaborate responsibility reporting or are too small to have an adequate separation of duties. (Incorrect. This is a true statement. In many organizations, effective supervision takes the place of more expensive controls. Effective supervision involves training and assisting employees, monitoring their performance, correcting errors, and safeguarding assets by overseeing employees who have access to them.)

6. To achieve effective segregation of duties, certain functions must be separated. Which of the following is the correct listing of the accounting-related functions that must be segregated?
a. control, recording, and monitoring (Incorrect. See Figure 7-3.)
▶ b. authorization, recording, and custody (Correct. See Figure 7-3.)
c. control, custody, and authorization (Incorrect. See Figure 7-3.)
d. monitoring, recording, and planning (Incorrect. See Figure 7-3.)

7. Which of the following is NOT an independent check?
a. bank reconciliation (Incorrect. A bank reconciliation is an independent check, as are top-level reviews, analytical reviews, reconciling two independently maintained sets of records, comparisons of actual quantities with recorded amounts, double-entry accounting, and independent reviews.)
b. periodic comparison of subsidiary ledger totals to control accounts (Incorrect. A periodic comparison of subsidiary ledger totals to control accounts is an independent check, as are top-level reviews, analytical reviews, reconciling two independently maintained sets of records, comparisons of actual quantities with recorded amounts, double-entry accounting, and independent reviews.)
c. trial balance (Incorrect. A trial balance is an independent check, as are top-level reviews, analytical reviews, reconciling two independently maintained sets of records,

comparisons of actual quantities with recorded amounts, double-entry accounting, and independent reviews.)

▶ d. re-adding the total of a batch of invoices and comparing it with your first total (Correct. One person performing the same procedure twice using the same documents, such as re-adding invoice batch totals, is not an independent check because it does not involve a second person, a second set of documents or records, or a second process.)

8. Which of the following is a control procedure relating to both the design and use of documents and records?
   a. locking blank checks in a drawer (Incorrect. Locking blank checks in a drawer is not a control procedure related to the design of documents.)
   b. reconciling the bank account (Incorrect. Reconciling the bank account is not a control procedure related to the design of documents.)
   ▶ c. sequentially prenumbering sales invoices (Correct. Designing documents so that they are sequentially prenumbered and then using them in order is a control procedure relating to both the design and use of documents.)
   d. comparing actual physical quantities with recorded amounts (Incorrect. Comparing actual quantities to recorded amounts is not a control procedure related to the design of documents.)

9. Which of the following is the correct order of the risk assessment steps discussed in this chapter?
   ▶ a. Identify threats, estimate risk and exposure, identify controls, and estimate costs and benefits. (Correct. See Figure 7-2.)
   b. Identify controls, estimate risk and exposure, identify threats, and estimate costs and benefits. (Incorrect. See Figure 7-2.)
   c. Estimate risk and exposure, identify controls, identify threats, and estimate costs and benefits. (Incorrect. See Figure 7-2.)
   d. Estimate costs and benefits, identify threats, identify controls, and estimate risk and exposure. (Incorrect. See Figure 7-2.)

10. Your current system is deemed to be 90% reliable. A major threat has been identified with an impact of $3,000,000. Two control procedures exist to deal with the threat. Implementation of control A would cost $100,000 and reduce the likelihood to 6%. Implementation of control B would cost $140,000 and reduce the likelihood to 4%. Implementation of both controls would cost $220,000 and reduce the likelihood to 2%. Given the data, and based solely on an economic analysis of costs and benefits, what should you do?
   a. Implement control A only. (Incorrect. Control procedure A provides a net benefit of only $20,000, whereas control procedure B provides a net benefit of $40,000.)
   ▶ b. Implement control B only. (Correct. Control procedure B provides a net benefit of $40,000. Procedure A and the combination of A and B provide a benefit of only $20,000.)
   c. Implement both controls A and B. (Incorrect. The combination of procedures A and B provides a net benefit of only $20,000, whereas control procedure B provides a net benefit of $40,000.)
   d. Implement neither control. (Incorrect. Both controls provide a net benefit. Control procedure B provides a net benefit of $40,000. Procedure A and the combination of A and B each provide a net benefit of $20,000.)

Expected loss = Impact × Likelihood ($300,000 = $3,000,000 × 10%)

Control Procedure	Likelihood	Impact	Revised Expected Loss	Reduction in Expected Loss	Cost of Control(s)	Net Benefit (Cost)
A	0.06	$3,000,000	$180,000	$120,000	$100,000	$20,000
B	0.04	$3,000,000	$120,000	$180,000	$140,000	$40,000
Both	0.02	$3,000,000	$ 60,000	$240,000	$220,000	$20,000