Chapter 11

Introduction to Internal Control Systems

After reading this chapter, you will:

1. *Be familiar with* the primary control frameworks commonly used in organizations.
2. *Be familiar with* an internal control system and the components of this system.
3. *Understand* the importance of enterprise-wide risk assessment and the impact this has on internal controls.
4. *Be familiar with* the importance of COSO and COBIT with respect to internal control systems.
5. *Understand* the difference between preventive, detective, and corrective controls.
6. *Be aware of* some of the control activities that should be included in an organization's internal control system.
7. *Understand* the reason an organization might be willing to let customers shoplift some of its merchandise inventory.

"Ultimately, all stakeholders in the company should share the same high-level goal of establishing a strong system of internal controls."

Robert Mueller, ''Mending Broken Controls,'' *Internal Auditor* (August 2008), p. 85.

INTRODUCTION

Protecting the assets of an organization has always been an important responsibility of management. However, the incredible advancements in IT, as well as the pervasive use of IT across firms of all sizes, have dramatically changed how managers establish and monitor internal controls. Indeed, the pervasiveness of IT also has a profound impact on internal and external auditors, and how they assess the strength of the internal control environment. Protecting such assets requires organizations to develop and implement an effective internal control system—a system that can also perform such other functions as helping ensure reliable data processing and promoting operational efficiency in an organization.

This chapter and the next cover the topic of internal controls—i.e., the controls established to protect the assets of an organization. This chapter defines corporate governance, IT governance, and internal controls. We also identify the components of an internal control system, the different types of controls, and various control activities. Finally, we illustrate a cost-benefit analysis, which is a method managers use to determine which control procedures are cost effective.

INTERNAL CONTROL SYSTEMS

An internal control system consists of the various methods and measures designed into and implemented within an organization to achieve the following four objectives: (1) safeguard assets, (2) check the accuracy and reliability of accounting data, (3) promote operational efficiency, and (4) enforce prescribed managerial policies. An organization that achieves these four objectives is typically one with good **corporate governance**. This means managing an organization in a fair, transparent, and accountable manner to protect the interests of all the stakeholder groups.[1] The 1992 COSO Framework is widely used by managers to organize and evaluate their corporate governance structure. This framework was developed to improve the quality of financial reporting through business ethics, effective internal controls, and corporate governance.[2]

Definition of Internal Control

Internal control describes the policies, plans, and procedures implemented by management of an organization to protect its assets. Usually the people involved in this effort are the entity's board of directors, the management, and other key personnel in the firm.

[1]''Corporate Governance: The New Strategic Imperative,'' a White Paper from the Economist Intelligence Unit, sponsored by KPMG International, http://www.eiu.com.
[2]Source: http://www.coso.org.

The reason this is important is that these individuals want reasonable assurance that the goals and objectives of the organization can be achieved (i.e., effectiveness and efficiency of operations, reliability of financial reporting, protection of assets, and compliance with applicable laws and regulations).[3]

Figure 11-1 identifies key laws, professional guidance, and reports that focus on internal controls.

In 2001, the AICPA issued Statement on Auditing Standards **(SAS) No. 94**, ''The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit.'' This SAS cautions the external auditors that the way firms use IT might impact any of the five internal control components (discussed in the next section). That is, auditors must realize internal controls are both manual and automated, and therefore, auditors might need to adopt new testing strategies to obtain sufficient evidence that an organization's controls are effective. Because of the complexity of IT environments, auditors will most likely need to use computer-assisted auditing techniques (CAATs) to test the automated controls in an organization. We discuss these techniques in depth in Chapter 14.

An important piece of legislation with respect to internal controls is the **Sarbanes-Oxley Act of 2002**. One key provision of this law is **Section 404**, which reaffirms that management is responsible for establishing and maintaining an adequate internal control structure, and at the end of each fiscal year must attest to the effectiveness and completeness of the internal control structure, thus making managers personally liable for this structure within the firm. We cover the Sarbanes-Oxley Act in more depth in Chapter 14.

1992 COSO Report—Components of Internal Control

The **1992 COSO Report** (see Figure 11-1) is important because it established a common definition of internal control for assessing control systems, as well as determined how to improve controls. According to the report, controls can serve many important purposes, and for this reason many businesses look at internal control systems as a solution to a variety of potential problems (such as dealing with rapidly changing economic and competitive environments, as well as shifting customer demands and priorities). According to the COSO report, an internal control system should consist of these five components: (1) the control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring.

Control Environment. The **control environment** establishes the tone of a company and influences the control awareness of the company's employees. It is the foundation for all the other internal control components and provides discipline and structure. Factors include:

- the integrity, ethical values, and competence of an organization's employees
- management's philosophy and operating style
- the way management assigns authority and responsibility as well as organizes and develops its employees
- the attention and direction provided by the board of directors

[3]Committee of Sponsoring Organizations of the Treadway Commission (CSOTC), *Internal Control—Integrated* Framework (COSO Report), 1992.

Date	Act/Report	Significant Provisions Pertaining to Internal Controls
1977	Foreign Corrupt Practices Act	• Requires publicly-owned companies to implement internal control systems • Only applies to publicly-owned corporations registered under Section 12 of the 1934 Securities and Exchange Act
1977	Treadway Commission Report	• Recommends development of a common definition for internal control, guidance for judging the effectiveness of internal control, and methods to improve internal controls
1988	SAS No. 55	• Management should establish an internal control structure that includes the following three components: the control environment, the accounting system, and the control procedures
1992	Committee of Sponsoring Organizations (COSO) Report	• Title: *Internal Control—Integrated Framework* • Defines internal control and describes its components • Presents criteria to evaluate internal control systems • Provides guidance for public reporting on internal controls • Offers materials to evaluate an internal control system
1992	COBIT—Control Objectives for Business and IT	• A Framework (set of best practices) for IT management • Provides managers, auditors, and IT users a set of generally accepted measures, indicators, processes, and best practices to maximize the benefits of IT and develop appropriate IT governance and control
1995	SAS No. 78	• Replaces definition of internal control structure in SAS No. 55 with the definition of internal control given in the 1992 COSO report
2001	SAS No. 94	• Provides guidance to auditors about the effect of IT on internal controls • Describes benefits and risks of IT to internal controls and how IT affects the components of internal controls
2002	Sarbanes-Oxley Act, Section 404	• Requires publicly-traded companies to issue an ''internal control report'' that states management is responsible for establishing and maintaining an adequate internal control structure • Management must assess the effectiveness of internal controls annually • The independent auditor for the firm must attest to and report on managements' assessment annually
2004	Committee of Sponsoring Organizations (COSO) Report	• Focuses on enterprise risk management • Includes the five components of ICIF (control environment, risk assessment, control activities, information and communication, and monitoring) and adds three components: objective setting, event identification, and risk response
2005	COBIT, Ver. 4.0	• Includes 34 high-level objectives that cover 215 control objectives categorized in four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate
2006	SAS No. 112	• Establishes standards and provides guidance to auditors of non-public entities on communicating matters related to an entity's internal control over financial reporting observed during a financial statement audit • To properly apply SAS No. 112, the auditor must have a working knowledge of the COSO framework
2007	COBIT, Ver. 4.1	• Better definitions of core concepts; improved control objectives • Application controls reworked; business and IT goals improved

FIGURE 11-1 Background information on internal controls.

Case-in-Point 11.1 A commonly-used source of information on reported cases of material weaknesses for publicly-traded companies is Audit Analytics (www.auditanalytics.com). One of the categories in this database is "senior management, tone, or reliability." A recent study of this particular category shows that audit firms issued adverse internal control opinions to 93 public companies (2005 to early 2008) because of weaknesses in "tone at the top."[4]

The personnel policies and practices that management adopts are an important aspect of the control environment. For example, an important control procedure is employee training programs that inform new hires about the company's various policies, outline individual responsibilities, and explain how to perform duties efficiently. Similarly, an organization should also conduct regular reviews of its operations to determine if they conform to desired operating policies. Many large and medium-sized enterprises have separate internal audit departments, whose internal auditors test existing internal controls for proper functioning and use. Small enterprises usually cannot afford their own internal audit departments, but they can hire outside consultants or ask managers to test compliance with operating policies.

Risk Assessment. It is not possible or even desirable to install controls for every possible risk or threat. The purpose of **risk assessment** is to identify organizational risks, analyze their potential in terms of costs and likelihood of occurrence, and implement only those controls whose projected benefits outweigh their costs. A general rule is: The more liquid an asset, the greater the risk of its misappropriation. To compensate for this increased risk, stronger controls are required. The COSO report recommends the use of a *cost-benefit analysis* (discussed and illustrated later in this chapter) to determine whether the cost to implement a specific control procedure is beneficial enough to spend the money. We expand on the topic of risk management in the next section.

Control Activities. These are the policies and procedures that the management of a company develops to help protect all of the different assets of the firm. Control activities include a wide variety of activities throughout the firm and are typically a combination of manual and automated controls. Some examples of these activities are approvals, authorizations, verifications, reconciliations, reviews of operating performance, and segregation of duties. Through properly designed and implemented *control procedures*, management will have more confidence that assets are being safeguarded and that the accounting data processed by the accounting system are reliable. This chapter provides several examples of control procedures, and also illustrates control activities that should be included in every company's internal control system.

Information and Communication. Managers must inform employees about their roles and responsibilities pertaining to internal control. This might include giving them documents such as *policies and procedures manuals* (discussed later) or posting memoranda on the company's intranet. This could also include training sessions for entry-level personnel and then annual refresher training for continuing employees. Regardless of the method, all employees need to understand how important their work is, how it relates to the work of other employees in the firm, and how that relates to strong internal controls. It is equally important that management understand the importance of keeping good working

[4]Hermanson, D., Ivancevich, D., and Ivancevich, S., "Tone at the Top," *Internal Auditor* (November 2008), pp. 39–45.

relationships between all layers of management so that employees feel safe communicating any possible problems they may find. When this is the case, employees at all levels can actually enhance the effectiveness of good internal controls. Also, they will be much more likely to point out any problems they may detect, and corrective action can be initiated.

Case-in-Point 11.2 Whistle-blowing systems help employees feel safe communicating problems or suspected wrongdoing to management. However, many potential whistleblowers continue to struggle with reporting problems that they witness because they are not sure how to report what they know, or fear possible consequences of doing so. One solution to this problem is to outsource the whistle-blower system—in fact, a recent survey of Chief Audit Executives reports that 60% of the organizations included in the survey have already outsourced their reporting systems."[5]

Monitoring. Evaluation of internal controls should be an ongoing process. Managers at various levels in the organization must evaluate the design and operation of controls and then initiate corrective action when specific controls are not functioning properly. This could include daily observations and scrutiny, or management might prefer regularly-scheduled evaluations. The scope and frequency of evaluations depend, to a large extent, on management's assessment of the risks the firm faces.

2004 COSO Report—Enterprise Risk Management

The 2004 COSO *Enterprise Risk Management – Integrated Framework* focuses on **enterprise risk management (ERM)** and builds upon the 1992 COSO *Internal Control – Integrated Framework* (ICIF). The ERM Framework (Figure 11-2) includes the five components of ICIF (control environment, risk assessment, control activities, information and communication, and monitoring) and adds three additional components: objective setting, event identification, and risk response.[6]

Objective Setting. ERM offers management a process for setting objectives for the firm—that is, the purposes or goals the firm hopes to achieve. ERM helps an organization determine if the objectives are aligned with the organizational strategy and that goals are consistent with the level of risk the organization is willing to take. An enterprise's objectives are viewed from four perspectives: (1) Strategic: the high-level goals and the mission of the firm, (2) Operations: the day-to-day efficiency, performance, and profitability of the firm, (3) Reporting: the internal and external reporting of the firm, and (4) Compliance: with laws and regulations.

Event Identification and Risk Response. Organizations must deal with a variety of uncertainties because many events are beyond the control of management. Examples include natural disasters, wars, unexpected actions of competitors, and changing conditions in the marketplace. However, it is critical for management to identify these external risks as quickly as possible and then consider internal and external factors regarding each event

[5]Baker, N., "See No Evil, Hear No Evil, Speak No Evil," *Internal Auditor* (April 2008), pp. 39–43.

[6]Sources: COSO website (www.erm.coso.org); F. Martens and L. Nottingham, Enterprise Risk Management: A Framework for Success, *RE: Business*, September 2003; and C. Chapman, Bringing ERM into Focus, *Internal Auditor Magazine*, June 2003.

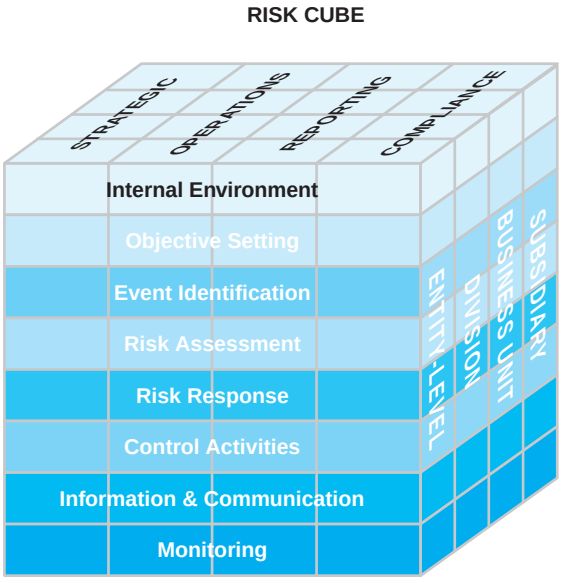

FIGURE 11-2 2004 COSO Enterprise Risk Management—Integrated Framework.

that might affect its strategy and achievement of objectives. Depending on the type or nature of events, management might be able to group some of them together and begin to detect trends that may help with risk assessment.

Case-in-Point 11.3 The responsibility of the Director of the Arkansas Department of Finance and Administration (DFA) is to ensure that state agencies operate uniformly and efficiently. To help the Director achieve these DFA objectives, each state agency is required to perform a risk assessment once every two years, and must complete a "Risk Assessment and Control Activities Worksheet."[7] This worksheet (Figure 11-3) helps department managers across the state to think about their operations through a risk-assessment lens.

The objective of risk assessment is to manage and control risk by identifying threats, analyzing the risks, and implementing cost-effective countermeasures to avoid, mitigate, or transfer the risks to a third party (through insurance programs). As they identify and categorize these risks, management will be in a better position to determine the probable effects on the organization. Management can then formulate and evaluate possible response options for the organization. In developing options, managers need to consider the level of risk they are willing to assume, as well as the trade-offs between costs and benefits of each choice. A number of computerized risk assessment software tools already exist to help managers with this task.

Case-in-Point 11.4 Managers need to ask themselves about the possible impact of certain risks—would it be minimal, significant, serious, or catastrophic?[8] RiskPAC, a business risk software solution, helps organizations detect and eliminate vulnerabilities in information systems and data security. CPACS, the company that developed RiskPAC, defines risk assessment as identification of the major risks and threats to which an organization's reputation, business

[7]Source: http://www.arkansas.gov/dfa/accounting/acc_ia_risk.html.
[8]Source: http://www.cpacsweb.com/riskpac.html (business continuity planning software products)

Risk Assessment and Control Activities Worksheet

Department: _____ Prepared By: _____

Activity: _____ Date Prepared: _____

Goals & Objectives	Risk Assessment			Actions to Manage Risks/ Control Activities
	Risks	Significance/Impact	Likelihood	
(1)	(2)	(3)	(4)	(5)

1 List all operations, financial reporting and compliance objectives associated with the activity. Goals should be clearly defined, measurable and attainable.

2 List all identified risks to the achievement of each goal and objective. Consider both internal and external risk factors. For each goal and objective, several different risks can be identified.

3 For each risk, estimate the potential impact on operations, financial reporting or compliance with laws and regulations, assuming that the risk occurs. Consider both quantitative and qualitative costs. Use **Large**, **Moderate** or **Small**.

4 For each risk, assess the likelihood of the risk occurring. Use **probable**, **reasonably possible**, or **remote**. Alternatively use **High**, **Medium** of **Low**.

5 For each risk with large or moderate impact and probable (high) or reasonable (medium) likelihood of occurrence, list both the actions to mitigate the risk to an acceptable level and the control activities that help ensure that those actions are carried out properly and in a timely manner. If no action is present to manage the risk and/or no control activity is present, an action plan to address the risk and an associated timeline should be included.

FIGURE 11-3 An example of a risk assessment and control activities worksheet.

Source: http://www.arkansas.gov/dfa/accounting/acc_ia_risk.html.

processes, functions, and assets are exposed. RiskPAC helps organizations determine the possibility that a harmful incident will occur (very likely, possible, probable, very unlikely).

2007 COBIT, Version 4.1[9]

The first edition of Control Objectives for Information and related Technology (COBIT) was issued in 1996, and the latest edition, version 4.1, was issued in 2007. The COBIT framework was created to be business focused, process oriented, controls based, and measurement driven. If we examine the mission statement for COBIT, we can quickly understand why this framework is widely used in corporate environments.

> *"To research, develop, publicize, and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals, and assurance professionals."*[10]

The COBIT framework takes into consideration an organization's business requirements, IT processes, and IT resources to support COSO requirements for the IT control environment. This suggests, rightfully so, that managers must *first* tend to the requirements outlined in the 1992 COSO Report and set up an internal control system that consists of these five components: (1) the control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The next step managers should take is to work through the guidelines contained in the 2004 COSO Report (perhaps using a worksheet like the one in Figure 11-3) to set objectives, identify possible risk events, and then consider appropriate risk responses the organization might need to take should an event occur.

Once the internal control system is in place (i.e., managers have worked through the 1992 and the 2004 COSO Frameworks), IT managers work with operational managers throughout the organization to determine how IT resources can best support the business processes. To achieve appropriate and effective governance of IT, senior managers of the organization will typically focus on five areas. First, managers need to focus on strategic alignment of IT operations with enterprise operations. Second, they must determine whether the organization is realizing the expected benefits (value) from IT investment. Third, managers should continually assess whether the level of IT investments is optimal. Fourth, senior management must determine their organization's risk appetite and plan accordingly. And finally, they must continuously measure and assess the performance of IT resources. Here again is an opportunity for managers to consider a ''dashboard'' to have access to key indicators of these five focus areas to support timely decision-making.

Perhaps it was the Sarbanes-Oxley Act, and the many governance lapses prior to the enactment of this legislation, that prompted the IT Governance Institute (ITGI) to recognize a need for and to develop a framework for IT governance. This governance framework, called Val IT, is a formal statement of principles and processes for IT management. **Val IT** is tightly integrated with COBIT. Although COBIT helps organizations understand if they are doing things right from an IT perspective, Val IT helps organizations understand if they are making the right investments and optimizing the returns from them. So, COBIT focuses on

[9]Source: IT Governance Institute, http://www.itgi.org.
[10]Source: IT Governance Institute, http://www.itgi.org.

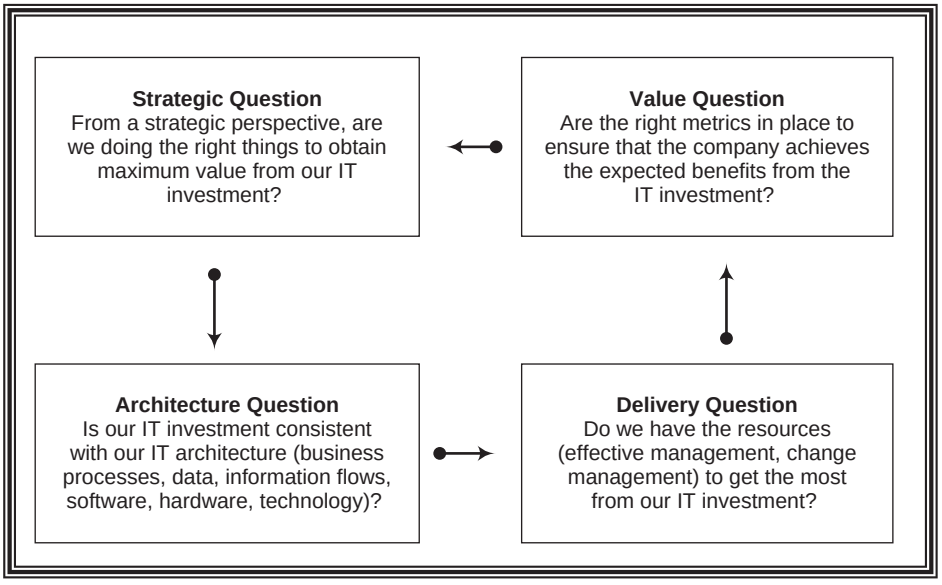

FIGURE 11-4 The integration of COBIT and Val IT.

Source: Adapted from the ISACA website (http://www.isaca.org).

the execution of IT operations, and Val IT focuses on the investment decision. Figure 11-4 diagrams the integration of COBIT and Val IT, which is described in considerable depth in ''The Val IT Framework 2.0 Extract.''[11] In essence, this is also a model for continuous improvement for an organization's IT governance program.

Val IT includes three very helpful publications that may be downloaded for free at the ISACA website (www.isaca.org), and these documents are: (1) Val IT Framework 2.0, (2) Val IT Getting Started with Value Management, and (3) Val IT The Business Case.

TYPES OF CONTROLS

A company's control procedures are often classified into three major types: *preventive controls, detective controls*, and *corrective controls*. This section examines each of these types of control procedures in more detail.

Preventive Controls

Preventive controls are controls that management puts in place to prevent problems from occurring. For example, a company might install a firewall to prevent unauthorized access to the company's network, thereby safeguarding the disclosure, alteration, or destruction of sensitive information from external hackers. Enterprise Risk Management (discussed earlier) helps managers identify areas where preventive controls should be in place. Under the section called ''Event Identification'' we said that management must identify possible

[11]Source: http://www.isaca.org.

events that represent a problem to the firm and then identify appropriate responses to those problems. James Cash calls this **scenario planning**, and it means management identifies scenarios of minor concern to major disasters that could occur.[12] Management should include a number of informed individuals in these brainstorming sessions, such as the IS team, IT auditors, external auditors, and perhaps risk-management consultants. First, management documents each scenario. Then, management must establish preventive controls to minimize the likelihood of each problem they identify. As Cash points out, preventive controls are never fail-safe, so a firm always needs detective controls to help discover when preventive controls fail. We'll talk more about the relationship of these two controls later in this chapter.

Detective and Corrective Controls

Because preventive controls cannot stop every possible problem from occurring, organizations also need strong **detective controls** that alert managers when the preventive controls fail. As an example, assume that a company's information system prepares daily responsibility accounting performance reports for management that computes variations of actual production costs from standard production costs. If a significant variance occurs, a manager's report signals this problem and the manager can initiate corrective action. Examples of *detective security controls* are log monitoring and review, system audits, file integrity checkers, and motion detection.[13]

Organizations can initiate corrective action only if corrective controls are in place. A company establishes corrective controls to remedy problems it discovers by the detective controls. Let's assume, based on the above detective control example, that performance reports repeatedly disclose that the company's actual direct labor hours for production work significantly exceed the standard direct labor hours. A corrective control procedure might be training programs that teach employees to perform their job functions more efficiently and effectively.

Corrective controls are procedures a company uses to solve or correct a problem. An example of this type of corrective control procedure might be a change to the company's procedures for creating backup copies of important business files. More than ever before, companies realize the importance of this corrective control since 9/11 and the many natural disasters that have occurred over the past few years.

Case-in-Point 11.5 Faced with many instances of fraud, hotels considered possible corrective controls to protect themselves from litigation and protect their guests from identity theft, without sacrificing customer service. Let's assume a guest calls, claiming that she forgot to pick up her folio (the record of charges and payments). She politely asks the hotel's accounting department to fax a copy. Hotels used to oblige the customer and fax the folio, which of course includes such information as the guest's name, address, signature, and credit card number. This seems like a nice service to a customer, but what if the person who called was not the guest? Many hotels now use the following procedures: (1) computers do not print the entire credit card number on the folio, and (2) folios are not faxed to anyone for any reason. Instead, hotels typically mail a folio only to the address on the reservation.[14]

---

[12]James Cash, ''It's Reasonable to Prepare,'' *Information Week*, No. 654 (October 27, 1997), p. 142.
[13]Source http://www.giac.org/resources/whitepaper/operations/207.php.
[14]Michael Barrier, ''Unmasking Hotel Fraud,'' *Internal Auditor*, Vol. 58 (April 2001), p. 28.

Interrelationship of Preventive and Detective Controls

Management should not treat preventive control procedures and detective control procedures separately. As we discussed earlier, these two controls work together to protect a company's internal control system.

CONTROL ACTIVITIES

Because each organization's accounting system is unique, there are no standardized control procedures that will work for every company. This means that each organization designs and implements specific controls based on its particular needs. However, certain control activities are common to every organization's internal control system. The ones that we will examine here are: (1) a good audit trail, (2) sound personnel policies and practices, (3) separation of duties, (4) physical protection of assets, (5) internal reviews of controls, and (6) timely performance reports.

Good Audit Trail

The basic inputs to an organization's AIS are business transactions that are monetarily measured. Organizations must keep an **audit trail** (initially discussed in Chapter 1) of these transactions within the organization's AIS. A good audit trail enables managers and auditors to follow the path of the data recorded in transactions from the initial source documents (for instance, a sales invoice) to the final disposition of the data on a report. In addition, managers and auditors can trace data from transactions on reports (such as expenses on an income statement) back to the source documents. In both of these processes, individuals can verify the accuracy of recorded business transactions. Without a good audit trail, errors and irregularities are more likely to happen and not be detected. To establish its audit trail, a company needs a *policies and procedures manual*. These documents should include the following items:

- A chart of accounts that describes the purpose of each general ledger account so that employees enter the debits and credits of accounting transactions in the correct accounts.
- A complete description of the types of source documents individuals must use to record accounting transactions. Also, include the correct procedures to prepare and approve the data for these documents.
- A comprehensive description of the authority and responsibility assigned to each individual. For example, who authorizes credit limits to customers?

Sound Personnel Policies and Practices

The employees at every level of a company are a very important part of the company's system of internal control. This is becoming increasingly obvious as managers downsize and right-size their organizations to streamline operations and cut costs. Consequently, there are fewer employees and these employees have more responsibility and oversight than in the past. The obvious result is that the opportunity for misappropriation is greater than before.

In addition, the capabilities of a company's employees directly affects the quality of the goods and services provided by the company. In general, competent and honest employees are more likely to help create value for an organization. Employees work with organizational assets (e.g., handling cash, acquiring and issuing inventory, and using equipment). Competent and honest employees, coupled with fair and equitable personnel policies, lead to efficient use of the company's assets. Most organizations post their personnel policies and procedures on their website so that they are easily accessible to all employees at any time.

Case-in-Point 11.6 Employees at the University of Arizona have ready access to a wealth of information regarding the university's personnel policies by searching the Human Resources Policy Manual (HRPM). The HRPM is available on the university website and includes policies on employment, benefits, compensation, employee relations, training and employee development, and additional university policies (e.g., conflict of interest, code of research ethics, and others).[15]

In general, little can be done to stop employees who are determined to embarrass, harm, or disrupt an organization. For example, several employees may conspire (*collude*) to embezzle cash receipts from customers. But, companies can encourage ethical behavior among employees in several ways. First, review the rules and the Code of Conduct. A number of organizations have too many ''picky'' rules that employees do not understand. To avoid this type of problem, managers should create rules that make a positive contribution to the productivity and effectiveness of a company, and then explain the rationale for these rules to employees. Secondly, managers should always lead by example. Figure 11-5 identifies some examples of personnel policies that firms might adopt.

All employees should be required to take their earned vacations (personnel policy 6). This is important for two reasons. First, if an employee is embezzling assets from an organization, the employee will probably not want to take a vacation. When an individual must go on vacation, another employee performs that person's job responsibilities and this increases the likelihood of detecting an embezzlement. Second, required vacations help employees to rest, enabling them to return refreshed and ready to perform their job functions more efficiently.

1. Specific procedures for hiring and retaining competent employees.
2. Training programs that prepare employees to perform their organizational functions efficiently.
3. Good supervision of the employees as they are working at their jobs on a daily basis.
4. Fair and equitable guidelines for employees' salary increases and promotions.
5. Rotation of certain key employees in different jobs so that these employees become familiar with various phases of their organization's system.
6. Vacation requirement that all employees take the time off they have earned.
7. Insurance coverage on those employees who handle assets subject to theft (fidelity bond).
8. Regular reviews of employees' performances to evaluate whether they are carrying out their functions efficiently and effectively, with corrective action for those employees not performing up to company standards.

FIGURE 11-5 Examples of personnel policies that firms might adopt.

[15]Source: http://www.hr.arizona.edu/09_rel/clsstaffmanual.php.

For employees who handle assets susceptible to theft, such as a company's cash and inventory of merchandise, it is a good personnel policy (number 7) to obtain some type of insurance coverage on them. Many organizations obtain **fidelity bond** coverage (from an insurance company) to reduce the risk of loss caused by employee theft of assets. The insurance company investigates the backgrounds of the employees that an organization wants to have bonded. When an insurance company issues one of these bonds, it assumes liability (up to a specified dollar amount) for the employee named in the bond.

Separation of Duties

The purpose of **separation of duties** is to structure work assignments so that one employee's work serves as a check on another employee (or employees). When managers design and implement an effective internal control system, they must try to separate certain responsibilities. If possible, managers should assign the following three functions to different employees: *authorizing* transactions, *recording* transactions, and maintaining *custody of assets*.

Authorizing is the decision to approve transactions (e.g., a sales manager authorizing a credit sale to a customer). *Recording* includes functions such as preparing source documents, maintaining journals and ledgers, preparing reconciliations, and preparing performance reports. Finally, *custody of assets* can be either direct, such as handling cash or maintaining an inventory storeroom, or indirect, such as receiving customer checks through the mail or writing checks on a company's bank account. If two of these three functions are the responsibility of the same employee, problems can occur.

We describe three real-world cases that demonstrate the importance of separating duties. Immediately following each case is a brief analysis of the problem.

Case-in-Point 11.7 The controller of a Philippine subsidiary confessed to embezzling more than $100,000 by taking advantage of currency conversions. The controller maintained two accounts—one in Philippine pesos to deposit funds collected locally and the other account in U.S. dollars so he could transfer funds from the Philippine account to the US account. The auditor became suspicious when he noticed that each transfer was rounded to the nearest thousand in pesos and dollars. For example, one day the statements showed an $885,000 (pesos) transfer from the local-currency account and a transfer of exactly $20,000 into the U.S.-dollar account. Further investigation revealed that the controller was actually withdrawing cash from the peso account, keeping some of the money, and depositing only enough pesos in the U.S. currency account to show a transaction of exactly $20,000. Because the withdrawal and the deposit took place almost simultaneously, the U.S. controller never suspected any wrongdoing.[16]

Analysis. The control weakness here is that the controller had responsibility for both the *custody* of the cash (depositing the locally-collected funds in pesos) and the *recording* of the transactions (the deposit of the funds in the local account and the transfer of funds to the U.S. account). Consequently, he had control of the money throughout the process and was able to manipulate cash transfers to embezzle small amounts of money each time and then falsify the transactions that were recorded in each of the bank accounts to conceal the embezzlement activity.

Case-in-Point 11.8 The utilities director of Newport Beach, California, was convicted of embezzling $1.2 million from the city of Newport Beach over an 11-year period. The utilities

[16]Source: J. Mike Jacka, "Rounding Up Fraud," *Internal Auditor*, April 2001, p. 65.

director forged invoices or easement documents that authorized payments, for example, to real or fictitious city property owners for the rights to put water lines through their land. Officials within the Finance Department gave him the checks for delivery to the property owners. The utilities director then forged signatures, endorsed the checks to himself, and deposited them in his own accounts.

Analysis. The control weakness here is that the utilities director had physical *custody* of checks for the transactions he previously *authorized*. Due to the lack of separation of duties, the director could authorize fictitious transactions and subsequently divert the related payments to his own accounts.

Case-in-Point 11.9 The executive assistant (EA) to the president of a home improvement company used a corporate credit card, gift checks, and an online payment account to embezzle $1.5 million in less than three years. The EA arranged hotel and airline reservations and coordinated activities for the sales team. She was also responsible for reviewing the corporate credit card bills and authorizing payment. The president gave her the authority to approve amounts up to $100,000. When the EA realized that no one ever asked to look at the charges on the corporate credit card bill, she began making personal purchases with the card.[17]

Analysis. The control weakness here is that the EA was responsible for both *recording* the expenses and then *authorizing* payment of the bills. As a result, she quickly realized that she had nearly unlimited access to a variety of sources of funds from the company, and then found other ways to have the company pay for the things she wanted (i.e., gift checks and a Paypal account that she set up).

The *separation of duties* concept is very important in IT environments. However, the way this concept is applied in these environments is often different. In today's information systems, for example, the computer can be programmed to perform one or more of the previously mentioned functions (i.e., authorizing transactions, recording transactions, and maintaining custody of assets). Thus, the computer replaces employees in performing the function (or functions). For example, the pumps at many gas stations today are designed so that customers can insert their debit or credit cards to pay for their gas. Consequently, the computer performs all three functions: authorizes the transaction, maintains custody of the ''cash'' asset, and records the transaction (and produces a receipt if you want one).

Physical Protection of Assets

A vital control activity that should be part of every organization's internal control system is the physical protection of its assets. Beyond simple protection from the elements, the most common control is to establish accountability for the assets with custody documents. Three application areas for this are (1) inventory controls, (2) document controls, and (3) cash controls.

Inventory Control. To protect inventory, organizations keep it in a storage area accessible only to employees with custodial responsibility for the inventory asset. Similarly, when purchasing inventory from vendors, another procedure is to require that each shipment of inventory be delivered directly to the storage area. When the shipment arrives, employees prepare a *receiving report* source document. This report, as illustrated in Figure 11-6, provides documentation about each delivery, including the date received,

[17]Source: Paul Sutphen, ''Stealing Funds for a Nest Egg,'' *Internal Auditor*, (August 2008), pp. 87–91.

Sarah's Sporting Goods
Receiving Report
No. 7824

Vendor: Richards Supply Company	**Date Received:** January 26, 2010
Shipped via: UPS	**Purchase Order Number:** 4362

Item Number	Quantity	Description
7434	100	Spalding basketballs
7677	120	Spalding footballs
8326	300	Spalding baseballs
8687	600	Penn tennis balls

Remarks:
Container with footballs received with water damage on outside, but footballs appear to be okay.

Received by:	Inspected by:	Delivered to:
Mark Langley	Mark Langley	Judy Phillips

FIGURE 11-6 Example of receiving report (items in boldface are preprinted).

vendor, shipper, and purchase order number. For every type of inventory item received, the receiving report shows the item number, the quantity received (based on a count), and a description.

The receiving report also includes space to identify the employee (or employees) who received, counted, and inspected the inventory items, as well as space for remarks regarding the condition of the items received. By signing the receiving report, the inventory clerk (Mark Langley in Figure 11-6) formally establishes responsibility for the inventory items. Any authorized employee can request inventory items from the storage area (for instance, to replenish the shelves of the store) and is required to sign the inventory clerk's *issuance report*, which is another source document. The clerk is thereby relieved of further responsibility for these requisitioned inventory items.

Document Control. Certain organizational documents are themselves valuable and must therefore be protected. Examples include the corporate charter, major contracts with other companies, blank checks (the following case-in-point), and registration statements required by the Securities and Exchange Commission. For control purposes, many organizations keep such documents in fireproof safes or in rented storage vaults offsite.

Case-in-Point 11.10 The Finance Office in Inglewood, California did not have adequate controls over important documents. As a result, a janitor who cleaned the Finance Office had access to blank checks that were left on someone's desk. The janitor took 34 blank checks,

forged the names of city officials, and then cashed them for amounts ranging from $50,000 to $470,000.

Organizations that maintain physical control over blank checks may still be at risk of embezzlement. You might be wondering how this could happen—it's due to the fact that so many banking transactions are electronic, and the method is known as a **demand draft**. If you write a check to your 12-year-old babysitter, she has all the information needed to clean out your account, because all she needs is your account number and bank routing number. Originally, demand drafts were used to purchase items over the phone (i.e., from telemarketers). Now, they're commonly used to pay monthly bills by having money debited automatically from an individual's checking account. Not surprisingly, due to the limited amount of information needed to make a demand draft, the potential for fraud is substantial. The irony of the demand draft system is that it may mean that paper checks are ultimately more risky to use than e-payments.

Case-in-Point 11.11 The Urban Age Institute, a nonprofit organization that focuses on planning new urban sustainability initiatives, received an email from a would-be donor who asked for instructions on how to wire a $1,000 donation into the agency's account. Not thinking anything unusual about the request, the group sent its account numbers. The "donor" used this information to print $10,000 worth of checks, which the "donor" cashed and then used Western Union to wire the money to her new Internet boyfriend in Nigeria. The Director at the Institute later discovered that the "donor" used the Institute's account number and bank routing number to obtain checks at Qchex.com. Fortunately, the Institute discovered the fraud and was able to close its checking account before money was withdrawn to cover the $10,000 in checks, which had already been deposited into the donor's Bank of America account.[18]

Cash Control. Probably the most important physical safeguards are those for cash. This asset is the most susceptible to theft by employees and to human error when employees handle large amounts of it. In addition to fidelity bond coverage for employees who handle cash, companies should also (1) make the majority of cash disbursements for authorized expenditures by check rather than in cash, and (2) deposit the daily cash receipts (either received in the mail from credit customers or through cash sales) intact at the bank.

If a company has various small cash expenditures occurring during an accounting period, it is usually more efficient to pay cash for these expenditures than to write checks. For good operating efficiency, an organization should use a *petty cash fund* for small, miscellaneous expenditures. To exercise control over this fund, one employee, called the *petty cash custodian*, should have responsibility for handling petty cash transactions. This employee keeps the petty cash money in a locked box and is the only individual with access to the fund.

Cash Disbursements by Check. A good audit trail of cash disbursements is essential to avoid errors and irregularities in the handling of cash. Accordingly, most organizations use pre-numbered checks to maintain accountability for both issued and unissued checks.

When paying for inventory purchases, there are two basic systems for processing vendor invoices: *nonvoucher systems* and *voucher systems*. Under a *nonvoucher* system, every approved invoice is posted to individual vendor records in the accounts payable file and then stored in an open invoice file. When an employee writes a cash disbursement check to pay an invoice, he or she removes the invoice from the open-invoice file, marks it

[18]Source: http://www.msnbc.msn.com/id/7914159/, Bob Sullivan, "Easy Check Fraud Technique Draws Scrutiny".

Sarah's Sporting Goods
Disbursement Voucher

No. 76742

Date Entered: February 9, 2010

Prepared by: GM

Vendor Number: 120

Remit to:
Valley Supply Company
3617 Bridge Road
Farmington, CT 06032

Debit Distribution	
Account No.	**Amount**
27-330	$750.00
27-339	450.00
28-019	300.00
29-321	425.00

Vendor Invoice					
Number	**Date**	**Amount**	**Returns & Allowances**	**Purchase Discount**	**Net Remittance**
4632	6/30/2010	$1250.00	$150.00	$22.00	$1078.00
4636	7/5/2010	675.00	0.00	13.50	661.50
Voucher Totals:		$1925.00	$150.00	$35.50	$1739.50

FIGURE 11-7 Example of disbursement voucher (items in boldface are preprinted).

paid, and stores it in the paid-invoice file. Under a *voucher* system, the employee prepares a *disbursement voucher* that identifies the specific vendor, lists the outstanding invoices, specifies the general ledger accounts to be debited, and shows the net amount to pay the vendor after deducting any returns and allowances as well as any purchase discount. Figure 11-7 illustrates a disbursement voucher.

As Figure 11-7 discloses, the disbursement voucher summarizes the information contained within a set of vendor invoices. When the company receives an invoice from a vendor for the purchase of inventory, an employee compares it to the information contained in copies of the *purchase order* and *receiving report* to determine the accuracy and validity of the invoice. An employee should also check the vendor invoice for mathematical accuracy. When the organization purchases supplies or services that do not normally involve purchase order and receiving report source documents, the appropriate supervisor approves the invoice.

A voucher system has two advantages over a non-voucher system: (1) it reduces the number of cash disbursement checks that are written, because several invoices to the same vendor can be included on one disbursement voucher, and (2) the disbursement voucher is an internally-generated document. Thus, each voucher can be pre-numbered to simplify the tracking of all payables, thereby contributing to an effective audit trail over cash disbursements.

Cash Receipts Deposited Intact. It is equally important to safeguard cash receipts. As an effective control procedure, an organization should *deposit intact* each day's accumulation of cash receipts at a bank. In the typical retail organization, the total cash

receipts for any specific working day come from two major sources: checks arriving by mail from credit-sales customers and currency and checks received from retail cash sales.

Because cash receipts are deposited intact each day, employees cannot use any of these cash inflows to make cash disbursements. Organizations use a separate checking account for cash disbursements. When organizations ''deposit intact'' the cash receipts, they can easily trace the audit trail of cash inflows to the bank deposit slip and the monthly bank statement. On the other hand, if employees use some of the day's receipts for cash disbursements, the audit trail for cash becomes quite confusing, thereby increasing the risk of undetected errors and irregularities.

Internal Reviews of Controls

As a result of the Sarbanes-Oxley Act (often referred to as SOX), the internal audit function of an organization typically reports directly to the Audit Committee of the Board of Directors. This makes the internal audit department independent of the other corporate subsystems and enhances objectivity when reviewing the operations of each subsystem. The internal audit staff makes periodic reviews, called **operational audits**, of each department (or subsystem) within its organization. These audits focus on evaluating the efficiency and effectiveness of operations within a particular department. Upon completion of such an audit, the internal auditors make recommendations to management for improving the department's operations.

A company's internal auditors may also be asked to perform a *fraud investigation* if managers suspect fraud within the organization. However, such an investigation requires specialized forensic accounting skills. If the audit department personnel do not have the requisite experience or skill to do such an investigation, the firm's external auditors may be able to help. In addition, internal auditors might need specialized information technology (IT) skills for their work, because they are often involved in IT auditing, which we discuss in Chapter 14.

In performing regular reviews of their company's internal control system, the internal auditors may find that certain controls are not operating properly. For example, the corporate policy manual might state that separate individuals should receive and record customer payments. However, that does not guarantee that this is what actually happens. If practice is not according to policy, it is the internal auditor's job to identify such problems and to inform management.

EVALUATING CONTROLS

Once controls are in place, it is a wise practice for management to evaluate them. We introduced several frameworks at the beginning of this chapter that companies might use to evaluate their internal controls, but regardless of *how* management chooses to evaluate their internal controls, it is clear that they *must* do this. Based on requirements contained in SOX, the New York Stock Exchange (NYSE) adopted rules that require all companies listed on this exchange to maintain an internal audit function to provide management and the audit committee ongoing assessments of the company's risk management processes and system of internal control.

Requirements of Sarbanes-Oxley Act

As previously discussed, the Sarbanes-Oxley Act of 2002 significantly changed the way internal auditors and management view internal controls within an organization. In particular, Section 404 contains very specific actions that the management of a publicly-traded company must perform each year with respect to the system of internal controls within the organization. Specifically, the annual financial report of the company must include a report on the firm's internal controls. This report must include the following:

- A statement that management acknowledges its responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting.
- An assessment, as of the end of the fiscal year, of the effectiveness of the internal control structure and procedures for financial reporting.
- An attestation by the company's auditor that the assessment made by the management is accurate.

A number of experts believe that some interesting synergies may have happened as a result of companies becoming SOX compliant. Recall that the purpose of SOX was to improve transparency and accountability in business processes and financial accounting. For this to happen, internal auditors and the management of companies had to study their processes very carefully. However, if these same firms already implemented an ERP, then most likely they already have reengineered some of their business processes to fit the ERP. During the evaluation of those processes, it is likely that the appropriate internal controls were considered and included, enabling SOX compliance. In addition, for management to comprehensively consider the requirements of SOX, they most likely used the Enterprise Risk Management framework in the 2004 COSO Report.

Illustrations of Cost-Benefit Analyses

Companies develop their own optimal internal control package by applying the cost-benefit concept. Under this concept, employees perform a cost-benefit analysis on each control procedure considered for implementation that compares the expected cost of designing, implementing, and operating each control to the control's expected benefits. Only those controls whose benefits are expected to be greater than, or at least equal to, the expected costs are implemented.

To illustrate a cost-benefit analysis, let's assume that the West End Boutique sells fashionable high-end ladies' clothing, jewelry, and other accessories. The owner is concerned about how much inventory customers have shoplifted during the last several months, and is considering some additional controls to minimize this shoplifting problem. If no additional controls are implemented, the company's accountant estimates that the total annual loss to the boutique from shoplifting will be approximately $120,000. The company is considering two alternative control procedures to safeguard the company's inventory (Figure 11-8).

Based on the owner's goal of reducing shoplifting, Alternative #1 (hiring six security guards) is the ideal control procedure to implement. Shoplifting should be practically zero, assuming that the guards are properly trained and perform their jobs in an effective manner. Even if shoplifting is completely eliminated, however, Alternative #1 should not be implemented. Why not? It costs too much. The control's expected cost ($240,000 a year) is greater than the control's expected benefit ($120,000 a year, which is the approximate annual shoplifting loss that would be eliminated).

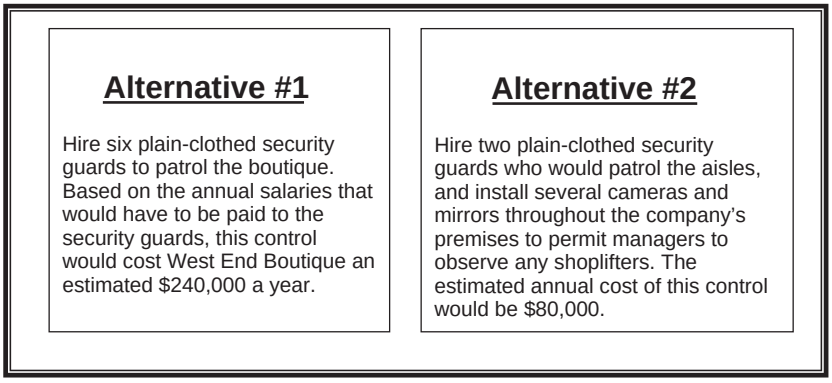

FIGURE 11-8 Internal control alternatives for West End Boutique.

If the owner implements Alternative #2 (hiring two security guards plus installing cameras and mirrors), the boutique's accountant estimates that the total annual loss from shoplifting could be reduced from $120,000 to $25,000. The net benefit is $95,000 (=$120,000—$25,000). Because the second alternative's expected benefit ($95,000 a year reduction of shoplifting) exceeds its expected cost ($80,000 a year), the boutique's owner should select Alternative #2.

The point of this cost-benefit analysis example is that in some situations, the design and implementation of an *ideal control procedure* may be impractical. We are using the term **ideal control** to mean a control procedure that reduces to practically zero the risk of an undetected error (such as debiting the wrong account for the purchase of office supplies) or irregularity (such as shoplifting). If a specific control's expected cost exceeds its expected benefit, as was true with the Alternative #1 control procedure discussed above, the effect of implementing that control is a decrease in operating efficiency for the company. From a cost-benefit viewpoint, therefore, managers are sometimes forced to design and implement control procedures for specific areas of their company that are less than ideal. These managers must learn to live with the fact that, for example, some irregularities may occur in their organizational system that will not be detected by the internal control system.

Another approach to cost-benefit analysis attempts to quantify the risk factor associated with a specific area of a company. *Risk assessment*, as discussed earlier, is an important component of an internal control system. In general, the benefits of additional control procedures result from reducing potential losses. A measure of loss should include both the *exposure* (that is, the amount of potential loss associated with a control problem) and the *risk* (that is, the probability that the control problem will occur). An example of a loss measure is **expected loss**, computed as follows:

$$\textbf{e}\text{xpected }\textbf{l}\text{oss} = \textbf{r}\text{isk} \times \textbf{e}\text{xposure}$$

The expected loss is based on estimates of risk and exposure. To determine the cost-effectiveness of a new control procedure, management estimates the expected loss both with and without the new procedure. On completing these calculations, the estimated benefit of the new control procedure is equal to the reduction in the estimated expected loss from implementing this procedure. Employees compare the estimated benefit to the incremental cost of the new control procedure. Whenever the estimated benefit exceeds this incremental cost, the company should implement the newly designed control procedure.

	Without Control Procedure	With Control Procedure	Net Expected Difference
Cost of payroll reprocessing	$10,000	$10,000	
Risk of data errors	15%	1%	
Reprocessing cost expected ($10,000 × risk)	$ 1,500	$ 100	$1,400
Cost of validation control procedure (an incremental cost)	$ 0	$ 600	$ (600)
Net estimated benefit from validation control procedure			$ 800

FIGURE 11-9 Cost-benefit analysis of payroll validation control procedure.

To demonstrate this method of cost-benefit analysis, assume that a company's payroll system prepares 12,000 checks biweekly. Data errors sometimes occur that require reprocessing the entire payroll at a projected cost of $10,000. The company's management is considering the addition of a data validation control procedure that reduces the error rate from 15% to 1%. This validation control procedure is expected to cost $600 per pay period. Should the data validation control procedure be implemented? Figure 11-9 illustrates the analysis to answer this question.

Figure 11-9 indicates that the reprocessing cost expected (=expected loss) is $1,500 without the validation control procedure and $100 with the validation control procedure. Thus, implementing this control procedure provides an estimated reprocessing cost reduction of $1,400. Because the $1,400 estimated cost reduction is greater than the $600 estimated cost of the control, the company should implement the procedure: the net estimated benefit is $800.

A Risk Matrix

Cost-benefit analyses suffer from at least three problems. One is that not all cost considerations can be expressed easily in monetary terms, and that *nonmonetary* (or *qualitative*) items are often as important in evaluating decision alternatives in a cost-benefit analysis. For example, when an airport contemplates whether or not to install a control that might save lives, it might be difficult to quantify the benefits. Admittedly, this is an extreme example, but the point remains: often qualitative factors exist in a decision-making situation, which requires a degree of subjectivity in the cost-benefit analyses.

Another problem with cost-benefit analyses is that some managers are not comfortable with computations involving probabilities or averages. What does it mean, for example, to state that on average 2.5 laptops are lost or stolen each year? Finally, a third problem with cost-benefit analyses is that they require an evaluation of all possible risks, and a case-by-case computation of possible safeguards. Typically, companies will run out of money for controls long before they run out of risks to mitigate.

A possible solution to this third problem is to develop a **risk matrix**, such as the one in Figure 11-10—a tool especially useful for prioritizing large risks. As you can see, a risk matrix classifies each potential risk by mitigation cost and also by likelihood of occurrence. As a result, highly-likely, costly events wind up in the upper-right corner of the matrix, and events with small likelihoods of occurrence or negligible costs wind up in the lower left corner. This helps managers see which events are most important (the upper-right ones), and therefore how to better prioritize the money spent on internal controls.

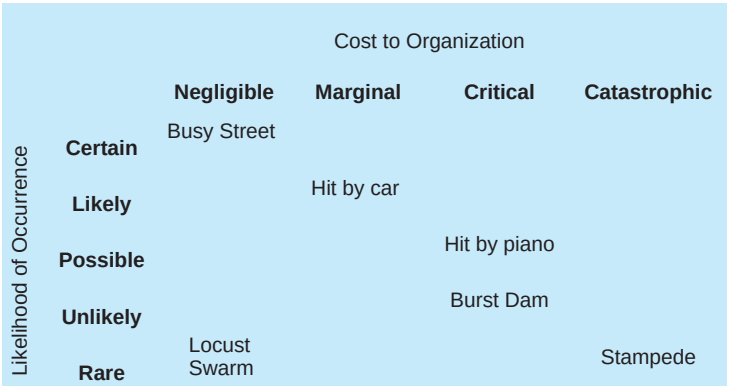

FIGURE 11-10 Example of a risk matrix.

AIS AT WORK
Using the Company Credit Card as a Nest Egg?[19]

Laura Jones, 22-years old, was very excited! She just got hired at a regional home improvement company as the executive assistant to the president. The company was eagerly planning an aggressive expansion of operations and was looking for ambitious and eager employees willing to work hard as team players. To realize growth, the president of the company knew they had to be very active in the industry, so the company sponsored booths at trade shows, attended industry conferences, and had morale-building events for its sales team in exciting places such as Hawaii.

Jones' responsibilities included making all the arrangements for these activities. She made hotel and airline reservations and coordinated activities for the sales team. She was also responsible for reviewing the corporate credit card bills and authorizing payments. The president gave her the authority to approve amounts up to $100,000. However, when Jones realized that no one ever asked to look at the charges on the corporate credit card bill, she began making personal purchases with the card. If total charges exceeded $100,000, she simply forged the president's signature on the approval form. When she learned that the accounts payable department accepted approvals from the president by email, she would slip into the president's office when he was at a meeting or out of town, access his computer, and send herself an ''approval'' email.

But the temptation was so great that she began to find additional ways the company could pay for things she wanted. For example, she soon discovered that she could also purchase gift checks with the corporate credit card, and over a two year period she bought more than $150,000 in gift checks to buy items for herself, her family, and some friends.

When Jones had been with the firm for slightly less than three years, her scheme was discovered. An agent at the credit card company noticed some questionable transactions involving Jones and the corporate credit card. When the internal auditors investigated the transactions, they discovered that Jones had embezzled more than $1.5 million.

[19]Source: Paul Sutphen, ''Stealing Funds for a Nest Egg,'' *Internal Auditor*, (August 2008), pp. 87–91.

SUMMARY

- An organization's internal control system has four objectives: (1) to safeguard assets, (2) to check the accuracy and reliability of accounting data, (3) to promote operational efficiency, and (4) to encourage adherence to prescribed managerial policies.
- It is management's responsibility to develop an internal control system.
- The control environment, risk assessment, control activities, information and communication, and monitoring are the five interrelated components that make up an internal control system.
- Six control activities to include in each organization's internal control system are: (1) a good audit trail, (2) sound personnel policies and practices, (3) separation of duties, (4) physical protection of assets, (5) internal reviews of controls by internal audit subsystem, and (6) timely performance reports.
- Within these six activities, specific control procedures should be designed and implemented for each company based on its particular control needs.
- To develop an optimal internal control package, management should perform a cost-benefit analysis on each potential control procedure.
- A company should only implement those controls whose expected benefits exceed, or at least equal, their expected costs.

KEY TERMS YOU SHOULD KNOW

audit trail
control activities
control environment
COBIT
corporate governance
corrective controls
COSO Report, 1992
COSO Report, 2004
demand draft
detective controls
enterprise risk management (ERM)
event identification
expected loss
fidelity bond
ideal control
internal control
objective setting
operational audits
preventive controls
risk assessment
risk matrix
risk response
SAS No. 94
scenario planning
separation of duties
SOX, Section 404
Val IT

TEST YOURSELF

Q11-1. This term describes the policies, plans, and procedures implemented by a firm to protect the assets of the organization.

a. Internal control

b. SAS No. 94

c. Risk assessment

d. Monitoring

Q11-2. Which of the following is not one of the four objectives of an internal control system?

a. Safeguard assets

b. Promote firm profitability

c. Promote operational efficiency

d. Encourage employees to follow managerial policies

Q11-3. Section 404 affirms that management is responsible for establishing and maintaining an adequate internal control structure. This Section may be found in which of the following?

a. The 1992 COSO Report

b. The 2004 COSO Report

c. The Sarbanes-Oxley Act of 2002

d. COBIT

Q11-4. Which of the following would a manager most likely use to organize and evaluate corporate governance structure?

a. The 1992 COSO Report

b. The 2004 COSO Report

c. The Sarbanes-Oxley Act of 2002

d. COBIT

Q11-5. Which of the following would a manager most likely use for risk assessment across the organization?

a. The 1992 COSO Report

b. The 2004 COSO Report

c. The Sarbanes-Oxley Act of 2002

d. COBIT

Q11-6. An internal control system should consist of five components. Which of the following is not one of those five components?

a. The control environment

b. Risk assessment

c. Monitoring

d. Performance evaluation

Q11-7. COSO recommends that firms _____ to determine whether they should implement a specific control.

a. Use cost-benefit analysis

b. Conduct a risk assessment

c. Consult with the internal auditors

d. Identify objectives

Q11-8. Which of the following is not one of the three additional components that was added in the 2004 COSO Report?

a. Objective setting

b. Risk assessment

c. Event identification

d. Risk response

Q11-9. Separation of duties is an important control activity. If possible, managers should assign which of the following three functions to different employees?

a. Analysis, authorizing, transactions

b. Custody, monitoring, detecting

c. Recording, authorizing, custody

d. Analysis, recording, transactions

DISCUSSION QUESTIONS

11-1. What are the primary provisions of the 1992 COSO Report? The 2004 COSO Report?

11-2. What are the primary provisions of COBIT?

11-3. Why are the COSO and COBIT frameworks so important?

11-4. Briefly discuss the interrelated components that should exist within an internal control system. In your opinion, which component is the most important and why?

11-5. Why are accountants so concerned about their organization having an efficient and effective internal control system?

11-6. Discuss what you consider to be the major differences between preventive, detective, and corrective control procedures. Give two examples of each type of control.

11-7. Why are competent employees important to an organization's internal control system?

11-8. How can separation of duties reduce the risk of undetected errors and irregularities?

11-9. Discuss some of the advantages to an organization from using a voucher system and pre-numbered checks for its cash disbursement transactions.

11-10. What role does cost-benefit analysis play in an organization's internal control system?

11-11. Why is it important for managers to evaluate internal controls?

PROBLEMS

11-12. You have been hired by the management of Alden, Inc. to review its control procedures for the purchase, receipt, storage, and issuance of raw materials. You prepared the following comments, which describe Alden's procedures.

- Raw materials, which consist mainly of high-cost electronic components, are kept in a locked storeroom. Storeroom personnel include a supervisor and four clerks. All are well trained, competent, and adequately bonded. Raw materials are removed from the storeroom only upon written or oral authorization from one of the production foremen.
- There are no perpetual inventory records; hence, the storeroom clerks do not keep records of goods received or issued. To compensate for the lack of perpetual records, a physical inventory count is taken monthly by the storeroom clerks, who are well supervised. Appropriate procedures are followed in making the inventory count.
- After the physical count, the storeroom supervisor matches quantities counted against a predetermined reorder level. If the count for a given part is below the reorder level, the supervisor enters the part number on a materials requisition list and sends this list to the accounts payable clerk. The accounts payable clerk prepares a purchase order for a predetermined reorder quantity for each part and mails the purchase order to the vendor from whom the part was last purchased.
- When ordered materials arrive at Alden, they are received by the storeroom clerks. The clerks count the merchandise and see that the counts agree with the shipper's bill of lading. All vendors' bills of lading are initialed, dated, and filed in the storeroom to serve as receiving reports.

a. List the internal control weaknesses in Alden's procedures.

b. For each weakness that you identified, recommend an improvement(s).

11-13. Listed below are 12 internal control procedures or requirements for the expenditure cycle (purchasing, payroll, accounts payable, and cash disbursements) of a manufacturing enterprise.

For each of the following, identify the error or misstatement that would be prevented or detected by its use.

a. Duties segregated between the cash payments and cash receipts functions

b. Signature plates kept under lock and key

c. The accounting department matches invoices to receiving reports or special authorizations before payment

d. All checks mailed by someone other than the person preparing the payment voucher

e. The accounting department matches invoices to copies of purchase orders

f. Keep the blank stock of checks under lock and key

g. Use imprest accounts for payroll

h. Bank reconciliations performed by someone other than the one who writes checks and handles cash

i. Use a check protector

j. Periodically conduct surprise counts of cash funds

k. Orders placed with approved vendors only

l. All purchases made by the purchasing department

11-14. Rogers, North, & Housour, LLC is a large, regional CPA firm. There are 74 employees at their Glen Allen, SC office. The administrative assistant at this office approached Mr. Rogers, one of the partners, to express her concerns about the inventory of miscellaneous supplies (e.g., pens, pencils, paper, floppy disks, and envelopes) that this office maintains for its clerical workers. The firm stores these supplies on shelves at the back of the office facility, easily accessible to all company employees.

The administrative assistant, Sandra Collins, is concerned about the poor internal control over these office supplies. She estimates that the firm loses about $350/month due to theft of supplies by company employees. To reduce this monthly loss, Sandra recommends a separate room to store these supplies, and that a company employee be given full-time responsibility for supervising the issuance of the supplies to those employees with a properly approved requisition. By implementing these controls, Sandra believes this change might reduce the loss of supplies from employee misappropriation to practically zero.

a. If you were Mr. Rogers, would you accept or reject Sandra's control recommendations? Explain why or why not.

b. Identify additional control procedures that the firm might implement to reduce the monthly loss from theft of office supplies.

11-15. Ron Mitchell is currently working his first day as a ticket seller and cashier at the First Run Movie Theater. When a customer walks up to the ticket booth, Ron collects the required admission charge and issues the movie patron a ticket. To be admitted into the theater, the customer then presents his or her ticket to the theater manager, who is stationed at the entrance. The manager tears the ticket in half, keeping one half for himself and giving the other half to the customer.

While Ron was sitting in the ticket booth waiting for additional customers, he had a ''brilliant'' idea for stealing some of the cash from ticket sales. He reasoned that if he merely pocketed some of the cash collections from the sale of tickets, no one would ever know. Because approximately 300 customers attend each performance, Ron believed that it would be difficult for the theater manager to keep a running count of the actual customers entering the theater. To further support his reasoning, Ron noticed that the manager often has lengthy conversations with patrons at the door and appears to make no attempt to count the actual number of people going into the movie house.

a. Will Ron Mitchell be able to steal cash receipts from the First Run Movie Theater with his method and not be caught? Explain.

b. If you believe he will be caught, explain how his stealing activity will be discovered.

11-16. The Palmer Company manufactures various types of clothing products for women. To accumulate the costs of manufacturing these products, the company's accountants have established a

computerized cost accounting system. Every Monday morning, the prior week's production cost data are batched together and processed. One of the outputs of this processing function is a production cost report for management that compares actual production costs to standard production costs, and computes variances from standard. Management focuses on the significant variances as the basis for analyzing production performance.

Errors sometimes occur in processing a week's production cost data. The cost of the reprocessing work on a week's production cost data is estimated to average about $12,000. The company's management is currently considering the addition of a data validation control procedure within its cost accounting system that is estimated to reduce the risk of the data errors from 16% to 2%, and this procedure is projected to cost $800/week.

a. Using these data, perform a cost-benefit analysis of the data validation control procedure that management is considering for its cost accounting system.

b. Based on your analysis, make a recommendation to management regarding the data validation control procedure.

CASE ANALYSES

11-17. Gayton Menswear (Risk Assessment and Control Procedures)

The Gayton Menswear company was founded by Fred Williams in 1986 and has grown steadily over the years. Fred now has 17 stores located throughout the central and northern parts of the state. Because Fred was an accounting major in college and worked for a large regional CPA firm for 13 years prior to opening his first store, he places a lot of value on internal controls. Further, he has always insisted on a state-of-the art accounting system that connects all of his stores' financial transactions and reports.

Fred employs two internal auditors who monitor internal controls and also seek ways to improve operational effectiveness. As part of the monitoring process, the internal auditors take turns conducting periodic reviews of the accounting records. For instance, the company takes a physical inventory at all stores once each year and an internal auditor oversees the process. Chris Domangue, the most senior internal auditor, just completed a review of the accounting records and discovered several items of concern. These were:

- Physical inventory counts varied from inventory book amounts by more than 5% at two of the stores. In both cases, physical inventory was lower.
- Two of the stores seem to have an unusually high amount of sales returns for cash.
- In 10 of the stores gross profit has dropped significantly from the same time last year.
- At four of the stores, bank deposit slips did not match cash receipts.
- One of the stores had an unusual number of bounced checks. It appeared that the same employee was responsible for approving each of the bounced checks.
- In seven of the stores, the amount of petty cash on hand did not correspond to the amount in the petty cash account.

Requirement

1. For each of these concerns, identify a risk that may have created the problem.
2. Recommend an internal control procedure to prevent the problem in the future.

11-18. Cuts-n-Curves Athletic Club (Analyzing Internal Controls)

The Cuts-n-Curves Athletic Club is a state-wide chain of full-service fitness clubs that cater to the demographics of the state (about 60% of all adults are single). The clubs each have an indoor swimming pool, exercise equipment, a running track, tanning booths, and a smoothie café for after-workout refreshments. The Club in Rosemont is open seven days a week, from 6:00 a.m. to 10:00 p.m. Just inside the front doors is a reception desk where an employee greets patrons. Members must present their membership card to be scanned by the bar-code reader, and visitors pay a $16 daily fee.

When the employee at the desk collects cash for daily fees, he or she also has the visitor complete a waiver form. The employee then deposits the cash in a locked box and files the forms. At the end of each day the Club accountant collects the cash box, opens it, removes the cash, and counts it. The accountant then gives a receipt for the cash amount to the employee at the desk. The accountant takes the cash to the bank each evening. The next morning, the accountant makes an entry in the cash receipts journal for the amount indicated on the bank deposit slip.

Susan Richmond, the General Manager at the Rosemont Club, has some concerns about the internal controls over cash. However, she is concerned that the cost of additional controls may outweigh any benefits. She decides to ask the organization's outside auditor to review the internal control procedures and to make suggestions for improvement.

Requirements:

1. Assume that you are the outside (staff) auditor. Your manager asks you to identify any weaknesses in the existing internal control system over cash admission fees.
2. Recommend one improvement for each of the weaknesses you identified.

11-19. Emerson Department Store (Control Suggestions to Strengthen a Payroll System)

As a recently hired internal auditor for the Emerson Department Store (which has approximately 500 employees on its payroll), you are currently reviewing the store's procedures for preparing and distributing the weekly payroll. These procedures are as follows.

- Each Monday morning the managers of the various departments (e.g., the women's clothing department, the toy department, and the home appliances department) turn in their employees' time cards for the previous week to the accountant (Morris Smith).
- Morris then accumulates the total hours worked by each employee and submits this information to the store's computer center to process the weekly payroll.
- The computer center prepares a transaction tape of employees' hours worked and then processes this tape with the employees' payroll master tape file (containing such things as each employee's social security number, exemptions claimed, hourly wage rate, year-to-date gross wages, FICA taxes withheld, and union dues deducted).
- The computer prints out a payroll register indicating each employee's gross wages, deductions, and net pay for the payroll period.
- The payroll register is then turned over to Morris, who, with help from the secretaries, places the correct amount of currency in each employee's pay envelope.

- The pay envelopes are provided to the department managers for distribution to their employees on Monday afternoon.

To date, you have been unsuccessful in persuading the store's management to use checks rather than currency for paying the employees. Most managers that you have talked with argue that the employees prefer to receive cash in their weekly pay envelopes so that they do not have to bother going to the bank to cash their checks.

Requirements:

1. Assume that the store's management refuses to change its current system of paying the employees with cash. Identify some control procedures that could strengthen the store's current payroll preparation and distribution system.
2. Now assume that the store's management is willing to consider other options for paying employees. What alternatives would you suggest?

REFERENCES AND RECOMMENDED READINGS

Campbell, D., M. Campbell, & G. Adams. ''Adding significant value with internal controls,'' *The CPA Journal* (June 2006), pp. 20–25.

Campbell, M., G. Adams, D. Campbell, & M. Rose. ''Internal audit can deliver more value,'' *Financial Executive* (Jan-Feb 2006), pp. 44–47.

Committee of Sponsoring Organizations of the Treadway Commission (CSOTC). *Enterprise Risk Management—Integrated Framework (COSO Report)*, New York: 2004.

Harrington, C. ''Internal audit's new role,'' *Journal of Accountancy* (September 2004), p. 65–70.

Jeffrey, C. ''From lemons to lemonade,'' *Risk Management* (July 2008), pp. 48–51.

Joseph, G. & T. Engle. ''The use of control self-assessment by independent auditors,'' *The CPA Journal* (December 2005), pp. 38–43.

Nolan, M. ''Internal audit at the crossroads,'' *Risk Management* (November 2008), pp. 54–55.

Shaw, J. & L. Garvin. ''ERM in motion,'' *Risk Management* (July 2006), pp. 24–29.

Singh, G. ''What can SOX do for you?'' *Risk Management* (April 2008), p. 78.

Thomson, J., ''SOX 404 and ERM: Perfect partners or not?'' *The Journal of Corporate Accounting & Finance* (March/April 2007), pp. 29–36.

Walker, K. ''SOX, ERP, and BPM,'' *Strategic Finance* (December 2008), pp. 47–53.

Wells, J. ''When the boss trumps internal controls,'' *Journal of Accountancy* (February 2006), pp. 55–57.

ANSWERS TO TEST YOURSELF

1. **a** 2. **b** 3. **c** 4. **a** 5. **b** 6. **d** 7. **a** 8. **b** 9. **c**