CHAPTER 7

CONTROLLING INFORMATION SYSTEMS: INTRODUCTION TO ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL

LEARNING OBJECTIVES

AFTER READING THIS CHAPTER, YOU SHOULD BE ABLE TO:

- SUMMARIZE THE EIGHT ELEMENTS OF COSO'S *ENTERPRISE RISK MANAGEMENT–INTEGRATED FRAMEWORK.*
- UNDERSTAND THAT MANAGEMENT EMPLOYS INTERNAL CONTROL SYSTEMS AS PART OF ORGANIZATIONAL AND IT GOVERNANCE INITIATIVES.
- DESCRIBE HOW INTERNAL CONTROL SYSTEMS HELP ORGANIZATIONS ACHIEVE OBJECTIVES AND RESPOND TO RISKS.
- DESCRIBE FRAUD, COMPUTER FRAUD, AND COMPUTER ABUSE.
- ENUMERATE CONTROL GOALS FOR OPERATIONS AND INFORMATION PROCESSES.
- DESCRIBE THE MAJOR CATEGORIES OF CONTROL PLANS.

The twenty-first century started with a bang! News of business scandals and corruption blazed across worldwide media at the speed of light. CPA firms, investors, lenders, managers, and innocent bystanders were deeply affected by the discovery, nature, and extent of corporate malfeasance. The direct injuries sustained by corporate stakeholders were staggering, and the collateral damage inflicted on the public was frightening. Reports of corporate shenanigans dominated newspaper headlines. These included the Enron Corporation, Arthur Andersen, WorldCom, Adelphia Communications, Tyco International, and Quest Communications.

These are but a few of the more notable business and audit failures uncovered in the early part of the twenty-first century. How did these situations occur and what would have prevented them? In response to these scandals, the U.S. Congress passed the Sarbanes-Oxley Act of 2002 (SOX) to mandate improved organizational governance. These improvements included auditor independence, composition and responsibilities of boards of directors and management, and enhanced financial disclosures. Of particular interest for our discussions in this chapter are the requirements related to internal

control. SOX section 404 required that management and auditors document, test, and report on the effectiveness of internal controls over financial reporting.

In complying with SOX, organizations improved decision making, obtained process efficiencies, engendered greater public confidence in their financial reporting, and improved their overall value. For example, studies have shown that better organizational governance has led to higher credit ratings and lower interests rates, which increase profits. These value improvements were in addition to regulatory compliance required by SOX and, hopefully, they reduce the chance of more frauds such as Enron. In this chapter, you will learn how organizational governance processes can improve organization performance and value while reducing fraud. You will see how COSO's *Enterprise Risk Management—Integrated Framework* can guide an organization's governance processes. And, finally, you will learn how *internal control*—a key component of governance and risk management—helps organizations achieve objectives, respond to risks, prevent fraud, and provide a means to detect fraud.

Synopsis

CONTROLS

ENTERPRISE SYSTEMS

Can an organization operate without good governance processes? Yes—but the chances of positive outcomes are much greater with governance processes that select objectives, establish processes to achieve the objectives, and monitor progress. Can these processes work toward achieving objectives without controls? Perhaps—but the odds are not very good! In this chapter, as well as in Chapters 8 and 9, we make the case that controlling business processes is a critically important element of organization governance and enterprise risk management. Controls provide reasonable assurance that objectives are achieved and that responses to risks are carried out. These chapters should provide you with a solid foundation for the later study of the controls for specific business processes that are covered in Chapters 10 through 15.

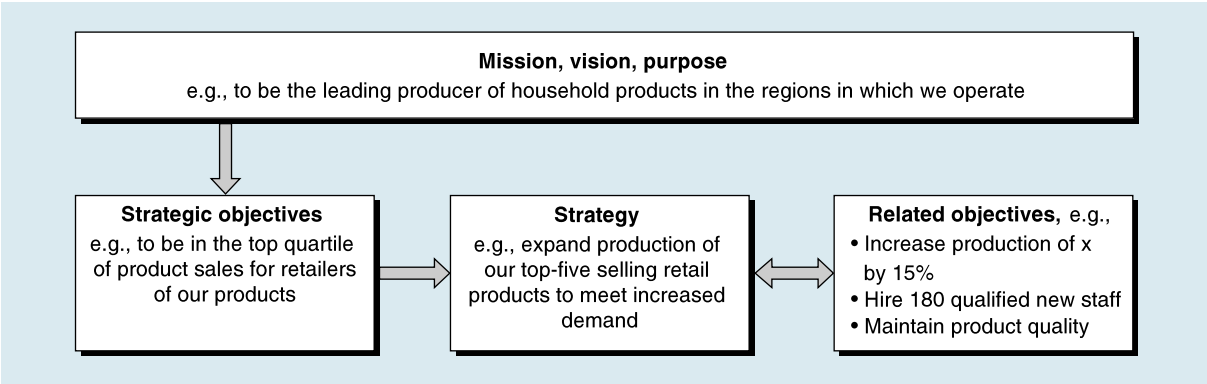
E-BUSINESS

We placed a Controls icon at the head of this synopsis to emphasize that the content of this chapter is almost entirely about controls. In this chapter, we consider the importance of controls in organizations that are tightly integrated internally, such as with *enterprise systems*, or have multiple connections to its environment, such as *e-business* architectures. Managers of these organizations must be confident that each component of the organization performs as expected; otherwise, chaos will prevail, and business partnerships will fail. In particular, organizations engaged in e-business must have internal control processes in place to reduce the possibilities of fraud and other disruptive events and to ensure compliance with applicable laws and regulations. For example, when engaged in Internet-based commerce, the organization may need to ensure the security of its own database, as well as the security of communication networks it operates in conjunction with trading partners; also, e-business firms might have to comply with relevant privacy-related laws and regulations. We begin by discussing organizational governance.

Organizational Governance

Organizational governance is a process by which organizations select objectives, establish processes to achieve objectives, and monitor performance. Objective setting includes defining mission, vision, purpose, and strategies to establish relationships such as those depicted in Figure 7.1. Processes to achieve the objectives (see "Related

FIGURE 7.1 Objective Setting



Source: Adapted from *Enterprise Risk Management—Integrated Framework, Application Techniques*, p. 20.

Objectives" in Figure 7.1), including essential internal controls and monitoring activities, are then designed and implemented. For example, production processes to produce product x—or increase its production—would be put in place, as would processes to screen and hire new staff and to acquire the raw materials that will be necessary for production. Finally, internal control and monitoring activities would be implemented—as separate functions or as part of these processes—to review performance and provide feedback to provide a reasonable assurance that objectives are being achieved. Has production increased by 15 percent? Did we hire 180 new staff, and are they qualified? Is quality being maintained?

Doesn't this seem to make sense? If you were running an organization, wouldn't you want to have objectives and relationships such as those depicted in Figure 7.1? Wouldn't you want to establish processes, controls, and monitoring mechanisms to see that your organization's objectives were being accomplished? Well, yes, but good governance isn't as easy in practice as it might sound. A quick search for definitions of governance should indicate the expansive nature of governance. For example, you might find descriptions that include "efficient management," "incentive mechanisms," "organization design, including the distribution of rights and responsibilities for managers, boards, and other stakeholders," "rules and procedures for making decision," "fairness, transparency, and accountability," and "return on investment/value creation." And so, we need guidance to implement an effective governance process. In the next section, we describe *Enterprise Risk Management*, a framework that has proven to be an effective process for organizational governance.

Enterprise Risk Management

"**Enterprise Risk Management (ERM)** is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may effect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the

EXHIBIT 7.1 Components of Enterprise Risk Management

- *Internal Environment:* The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- *Objective Setting:* Objectives must exist before management can identify potential events affecting their achievement. *Enterprise Risk Management* ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- *Event Identification:* Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- *Risk Assessment:* Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- *Risk Response:* Management selects risk responses—avoiding, accepting, reducing, or sharing risk—developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- *Control Activities:* Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- *Information and Communication:* Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- *Monitoring:* The entirety of ERM is monitored, and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Source: *Enterprise Risk Management—Integrated Framework, Executive Summary* (New York: The Committee of Sponsoring Organizations of the Treadway Commission, 2004): 5–6.

achievement of entity objectives."[1] The framework from which this definition is quoted[2] was developed to help management identify, assess, and manage risk. The ERM framework addresses four categories of management objectives:

- *Strategic:* High-level goals aligned with and supporting its mission.
- *Operations:* Effective and efficient use of its resources.
- *Reporting:* Reliability of reporting.
- *Compliance:* Compliance with applicable laws and regulations.[3]

The eight components that comprise the ERM framework are described in Exhibit 7.1.

The ERM process, and indeed the organizational governance process, begins with the first ERM component, *internal environment*, within which decisions are made about how an organization is to think about integrity, ethical values, risk (i.e., risk philosophy), how much risk they will be willing to accept (i.e., risk appetite), mechanisms for

1 *Enterprise Risk Management—Integrated Framework, Executive Summary* (New York: The Committee of Sponsoring Organizations of the Treadway Commission, 2004): 4.

2 The framework was issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, which studied the causal factors that can lead to fraudulent financial reporting. Five organizations comprise COSO: American Institute of CPAs (AICPA), American Accounting Association (AAA), Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA), and Financial Executives Institute (FEI).

3 *Enterprise Risk Management—Integrated Framework, Executive Summary* (New York: The Committee of Sponsoring Organizations of the Treadway Commission, 2004): 5.

oversight by the board of directors, organization design, and assignment of authority and responsibility. We can assume that this is the area in which the management at Enron, WorldCom, Adelphia, and others got started on the wrong foot.

After establishing its internal environment, an organization then moves on to *objective setting* (second ERM component) to define the relationships such as those depicted in Figure 7.1 (pg. 208). *Strategic* objectives are established as well as related objectives for *operations*, *reporting*, and *compliance*. Risk appetite guides strategy setting to balance, for example, growth, risk, and return. Risk appetite drives risk tolerances—acceptable levels of variation in achieving objectives. For example, the tolerance for the hiring objective in Figure 7.1 might be that we hire between 165 and 200 qualified new staff.

After an organization has its strategy and objectives in place, it must engage in *event identification* (third ERM component) to identify risks and opportunities that would affect achievement of its objectives. **Risks** are those events that would have a negative impact on organization objectives, and *opportunities* are events that would have a positive impact on objectives. Risks require assessment and response, whereas opportunities are channeled back to the strategy-setting process. For example, a new market opportunity might have opened up that management could decide to pursue.

After risks are identified, the organization must perform *risk assessment* (fourth ERM component) to determine the effect that risks may have on achievement of objectives. There are two factors to be considered: likelihood and impact. *Likelihood* is the possibility that an event will occur, and *impact* is the effect of an event's occurrence. For example, there might be a 75 percent chance that an event will occur, whereas the impact of the occurrence might be a loss of $50,000. Inherent risk exists in absence of any actions that management might take to reduce likelihood or impact. Exhibit 7.2 describes, with a little more detail, an approach to risk assessment.

In *risk response* (fifth ERM component), management selects from one of four response types. We can *avoid* a risk by leaving the activity that is giving rise to the risk. For example, if selling in a particular market poses unacceptable risk, we might get out of that market. We can *reduce* a risk by taking actions that reduce the likelihood of an event (e.g., institute fire-prevention programs) or reduce the impact (e.g., install sprinklers). We can *share* a risk by, for example, buying insurance or outsourcing the activity. Finally, we can *accept* a risk by taking no action (i.e., there is no cost/beneficial response). Residual risk is the risk that remains after one of these responses is chosen. Exhibit 7.3 (pg. 212) depicts the elements of a risk assessment and risk response process for a reporting objective, one of the related objective categories (see Figure 7.1 on pg. 208).

Control activities, the sixth ERM component, are policies and procedures that help ensure that risk responses are carried out. In some cases, the control is itself the risk response. Control activities, or simply controls, will be described later in this chapter and in Chapters 8 through 15. These controls include approvals, authorizations, verifications, reconciliations, reviews of operating performance, security procedures, and segregation of duties. The risk responses in Exhibit 7.3 are controls that seek to reduce the related risks.

The *information and communication* (seventh ERM component) component argues that pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication requires that appropriate, timely, and quality information from internal and external sources flows down, up, and across the entity to facilitate risk management and intelligent decision making. Personnel must understand their role in enterprise management and how individual activities relate to the work of others. For example, the

EXHIBIT 7.2 A Risk Assessment Process

How do we determine the possibility of sufficient *risk* that our objectives will not be achieved? A dilemma exists regarding the costs and benefits of risk responses. An organization strives to have enough control to ensure that its objectives are achieved. At the same time, the organization does not want to pay more for the controls than can be derived from their implementation. For example, suppose an organization installs a sophisticated fire-prevention and fire-detection system. This control should reduce the possibility of a fire destroying an organization's physical assets. If the fire-prevention system costs more than the assets being protected, however, the system obviously is not worthwhile from a financial perspective.

Many risk assessment models are used to determine whether a control should be implemented. As a practical matter, it is difficult to determine the amount to spend on a particular control or set of controls because an organization cannot afford to *prevent* all losses. One method that *can* be used is conceptually simple:

1. Estimate the annual dollar loss that would occur (i.e., the impact) should a costly event, say a destructive fire, take place. For example, say that the estimated loss is –$1,000,000.
2. Estimate the annual probability that the event will occur (i.e., the likelihood). Suppose the estimate is 5 percent.
3. Multiply item 1 by item 2 to get an initial *expected gross risk* (loss) of –$50,000 (–$1,000,000 x 0.05), which is the maximum amount or upper limit that should be paid for controls and the related risk reduction offered by such controls, in a given year. Next, we illustrate a recommendation plan using one *corrective* control, a fire insurance policy, and one *preventive* control, a sprinkler system.
4. Assume that the company would pay $1,000 annually (*cost of control*) for a $20,000 fire insurance policy (*reduced risk exposure due to control*). The estimated monetary damage remains at $1 million and *expected* gross risk (loss) remains at –$50,000 because there is still a 5 percent chance that a fire could occur. But, the company's *residual expected risk* exposure is now –$31,000 [–$50,000 + ($20,000 – $1,000)]. Our *expected* loss is reduced by the amount of the insurance policy (less the cost of the policy).
5. Next, you recommend that the company install a sprinkler system with a five-year annualized cost (net present value) of $10,000 each year to install and maintain (*cost of control*). At this point, you might be tempted to say that the company's *residual expected risk* just increased to –$41,000 (–$31,000 – $10,000), but wait! The sprinkler system lowered the likelihood of a damaging fire from 5 to 2 percent. In conjunction with this lower probability, the insurance company agreed to increase its coverage to $30,000 while holding the annual premium constant at $1,000.
6. Thus, the *residual expected risk* exposure is –$1,000, calculated as follows: Expected gross risk (–$20,000 or –$1,000,000 x 0.02) plus the insurance policy ($30,000) equals a gain of $10,000, but we must subtract the insurance premium ($1,000) and the sprinkler system ($10,000), leaving the residual expected risk at –$1,000.

Hence, *residual expected risk* is a function of *initial expected gross risk*, *reduced risk exposure due to controls*, and *cost of controls*. After all this, however, a large dose of management judgment is required to determine a *reasonable* level of control.

systems flowcharts introduced in Chapter 4 are an extremely effective means for depicting the actions and *control activities* related to each entity (e.g., person, department, computer) in a business process. With this information, personnel can appreciate their role in responding to risks and helping the organization achieve its objectives.

Monitoring is the eighth and final component of ERM, but it should not be considered a final activity. The ERM *process* and its components are evaluated—via ongoing management activities, separate evaluations, or both—to determine its effectiveness and to make necessary modifications. For example, business processes put in place to

EXHIBIT 7.3 Objectives, Risks, and Responses

Reporting Objective	Asset acquisitions and expenses entered for processing are valid, all entered (complete), and entered accurately.				
Target	Errors in monthly statements are less than $100,000.				
Tolerance	Errors less than $110,000.				
Risks	Inherent risk assessment		Risk response (examples)	Residual risk assessment	
	Likelihood	Impact		Likelihood	Impact
Vendors are paid from statements as well as invoices, resulting in duplicate payments (validity).	Possible	Minor $5,000–$15,000	Compare vendor name and number with those on file to detect duplicate invoices.	Unlikely	Minor $5,000–$7,500
Vendor invoices are not received prior to monthly cutoff (completeness).	Almost certain	Moderate $10,000–$25,000	Produce listings of unmatched POs (no invoice) and follow up.	Possible	Minor $2,500–$7,500
Vendor invoice amounts are captured incorrectly (accuracy).	Possible	Minor $5,000–$15,000	Programmed edits, including tests for blank fields and for reasonable quantities and amounts.	Unlikely	Minor $2,500–$7,500

Source: Adapted from *Enterprise Risk Management—Integrated Framework, Application Techniques* (New York: The Committee of Sponsoring Organizations of the Treadway Commission, 2004): 64.

accomplish objectives are reviewed to determine their effectiveness (e.g., has the output of the production process increased by 15 percent as indicated in Figure 7.1?). Controls implemented to respond to risks must be reviewed to determine that the activities have been performed and to determine whether additional actions must be taken to respond to the risk (e.g., has someone followed up on open POs as indicated in Exhibit 7.3 and is the residual risk as expected?). As a final example, the *event identification* process must be monitored to determine that evolving events have been identified and evaluated.

In conclusion, let's summarize ERM and revisit our initial proposition, that ERM is a process for *organizational governance*. ERM is a process, or framework, by which organizations create value for their stakeholders by establishing objectives and identifying and managing risks that might result in failure to achieve objectives. ERM is, therefore, a process for organizational governance. Now we move on to a discussion of SOX, the law the U.S. Congress responded with in reaction to the governance failures that manifested themselves at the start of the twenty-first century.

Sarbanes-Oxley Act

As a result of Enron, WorldCom, Tyco, and the other business scandals noted in the introduction to this chapter, the federal government was forced to interject its will into organizational governance. Why? Because these business entities failed to enact and enforce proper governance processes throughout their organizations, and as a result,

some employees boldly violated ethical codes, business rules, regulatory requirements, and/or statutory mandates, which resulted in massive frauds. Investors and lenders lost huge sums of money, and public trust in corporate managers, public accounting firms, and federal regulators had been severely, perhaps irreparably, harmed. The federal government's duty is to protect its citizens from such abuses; accordingly, one of the measures taken by Congress was to pass the Sarbanes-Oxley Act of 2002 (SOX), bringing about some of the largest changes to federal securities laws since the Securities Act of 1933 and the Securities Exchange Act of 1934.

This section is aimed at placing SOX into the context of organizational governance. We highlight SOX here—you will undoubtedly hear more about it in your financial accounting and auditing classes—because of the critical role that SOX has had in changing the way we design, implement, and evaluate systems of internal control. And, as noted previously, internal control is an essential element in managing the *risks* that may prevent achieving organizational objectives. The basic elements of SOX are outlined in Exhibit 7.4 (pgs. 214–215).

The key provisions of SOX are that SOX created a new accounting oversight board (the PCAOB), strengthened auditor independence rules, increased accountability of company officers and directors, mandated upper management to take responsibility for the company's internal control structure, enhanced the quality of financial reporting, and put teeth into white-collar crime penalties. Of particular note to students of accounting information systems, section 201 of the act prohibits audit firms from providing a wide array of nonaudit services to audit clients; in particular, the act prohibits consulting engagements involving the design and implementation of financial information systems. Does this suggest that CPA firms will no longer offer systems-related consulting engagements? No—it means that CPA firm A cannot offer such services to audit client X, but CPA firm B can provide these services to client X. Thus, in all likelihood, nonaudit engagements of this nature will swap around among CPA firms—not disappear altogether.

Section 404, which mandates the annual filing of an internal control report to the SEC, is of particular interest here as we introduce the concept of internal control. It is section 404 that has received the most press as companies and their auditors have struggled to comply with its requirements. To implement section 404, the PCAOB issued Auditing Standard No. 2 (AS2),[4] which requires that the management of each audited (i.e., publicly traded) company:

- Document significant processes, including the flow of transactions from initiation through recording and reporting, and related control activities.
- Identify the key controls that are in place to address the major risks related to financial reporting.
- Test key controls to determine their operating effectiveness.
- Present a written assessment of the effectiveness of internal control over financial reporting.

Subsequently, as part of the annual audit, each company's independent auditor must assess the management report and the company's system of internal control by:

- Evaluating and reporting on management's *process* for assessing the effectiveness of their internal controls.

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

- Independently testing and reporting about the effectiveness of the system of internal controls to determine that management's conclusions are correct.

To document processes, companies and their auditors use a variety of tools, including the narratives and *systems flowcharts* described in Chapter 4 of this text. To assess the effectiveness of the internal controls system design and to identify the controls to be tested to determine the operating effectiveness of the system of internal controls, companies and their auditors often use matrices such as those introduced later in this chapter and demonstrated in Chapters 9 through 15. These matrices match controls to the objectives that they purport to achieve.

Business process management (*BPM*) (see Technology Summary 2.4, pg. 41) often facilitates the implementation and assessment of a system of internal controls. With BPM, manual processes are automated, and all such processes perform consistently. The BPM engine handles the connections between processes to maintain the integrity of data moved among these processes. Management control policies are defined in the database

EXHIBIT 7.4 Outline of the Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (SOX) affects corporate managers, independent auditors, and other players who are integral to capital formation in the United States. This omnibus regulation will forever alter the face of corporate reporting and auditing. SOX titles and key sections are outlined here:

- *Title I—Public Company Accounting Oversight Board:* Section 101 establishes the Public Company Accounting Oversight Board (PCAOB), an independent board to oversee public company audits. Section 107 assigns oversight and enforcement authority over the board to the Securities and Exchange Commission (SEC).
- *Title II—Auditor Independence:* Section 201 prohibits a CPA firm that audits a public company to engage in certain nonaudit services with the same client. Most relevant to accounting information systems is the prohibition of providing financial information systems design and implementation services to audit clients. Section 203 requires audit partner rotation in their fifth, sixth, or seventh year, depending on the partner's role in the audit. Section 206 states that a company's chief executive officer (CEO), chief financial officer (CFO), controller, or chief accountant cannot have been employed by the company's audit firm and participated in an audit of that company during the prior one-year period.
- *Title III—Corporate Responsibility:* Section 302 requires a company's CEO and CFO to certify quarterly and annual reports. They are certifying that they reviewed the reports; the reports are not materially untruthful or misleading; the financial statements fairly reflect in all material respects the financial position of the company; and they are responsible for establishing, maintaining, and reporting on the effectiveness of internal controls, including significant deficiencies, frauds, or changes in internal controls.
- *Title IV—Enhanced Financial Disclosures:* Section 404 requires each annual report filed with the SEC to include an internal control report. The report shall state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and contain an assessment, as of the end of the company's fiscal year, of the effectiveness of the internal control structure and procedures of the company for financial reporting. The company's independent auditors must attest to and report on the assessments made by company management, and this attestation must be part of the regular financial statement audit, not a separate engagement. Section 406 requires that companies disclose whether or not they have adopted a code of ethics for senior financial officers. Section 407 requires that companies disclose whether or not their audit committee contains at least one member who is a financial expert. Section 409 requires that companies disclose information on material changes in their financial condition or operations on a rapid and current basis.
- *Title V—Analysts Conflicts of Interests:* Requires financial analysts to properly disclose in research reports any conflicts of interest they might hold with the companies they recommend.

(continued)

EXHIBIT 7.4 Outline of the Sarbanes-Oxley Act of 2002 *(continued)*

- *Title VI—Commission Resources and Authority:* Section 602 authorizes the SEC to censure or deny any person the privilege of appearing or practicing before the SEC if that person is deemed to be unqualified, have acted in an unethical manner, or have aided and abetted in the violation of federal securities laws.
- *Title VII—Studies and Reports:* Authorizes the General Accounting Office (GAO) to study the consolidation of public accounting firms since 1989 and offer solutions to any recognized problems.
- *Title VIII—Corporate and Criminal Fraud Accountability:* Section 802 makes it a felony to *knowingly* destroy, alter, or create records and/or documents with the intent to impede, obstruct, or influence an ongoing or contemplated federal investigation. Section 806 offers legal protection to whistleblowers who provide evidence of fraud. Section 807 provides criminal penalties of fines and up to 25 years imprisonment for those who knowingly execute, or attempt to execute, securities fraud.
- *Title IX—White-Collar Crime Penalty Enhancements:* Section 906 requires that CEOs and CFOs certify that information contained in periodic reports fairly presents, in all material respects, the financial condition and results of the company's operations. The section sets forth criminal penalties applicable to CEOs and CFOs of up to $5 million and up to 20 years in prison if they knowingly or willfully falsely so certify.
- *Title X—Corporate Tax Returns:* Section 1001 conveys a "sense of the Senate" that the corporate federal income tax returns are signed by the CEO.
- *Title XI—Corporate Fraud and Accountability:* Section 1102 provides for fines and imprisonment of up to 20 years to individuals who corruptly alter, destroy, mutilate, or conceal documents with the intent to impair the document's integrity or availability for use in an official proceeding, or to otherwise obstruct, influence, or impede any official proceeding. Section 1105 authorizes the SEC to prohibit anyone from serving as an officer or director if the person has committed securities fraud.

Source: 107 P.L. 204, § 1, 116 Stat. 745, July 30, 2002.

of business rules, and these rules are executed consistently, which leaves an audit trail of activities to demonstrate that the controls were performed. This latter feature helps both management and auditors in their assessment of the operating effectiveness of the system of internal controls and provides evidence of compliance with rules and regulations.

How has the implementation of SOX section 404 affected the performance of organizations and their systems of internal controls? The answer depends on who you talk to and their frame of reference. One study reports that first-year SOX section 404 costs averaged $1.5 million for smaller companies (market capitalization between $75 million and $700 million) and $7.3 million for larger companies.[5] Another asserts that the total costs for SOX in 2006 will exceed $6 billion.[6] On the other side of the issue, we see reports that companies have used information obtained during their SOX 404 compliance activities to improve processes, reduce risks, and build better businesses. Indeed, compliance efforts have revealed weaknesses in controls and business processes, and organizations have taken these findings and corrected problems, optimized their system of internal control, and improved processes. Investors have observed and acted on SOX 404 reports. For example, one report showed that the average share price gain of companies that had corrected internal control problems—from 2004 to 2005—exceeded

5 "Sarbanes-Oxley Section 404 Cost and Implementation Issues: Survey Update." Washington, DC: CRA International, December 8, 2005.

6 Kevin Reilly, "AMR Research Estimates Sarbanes-Oxley Spending Will Exceed $6 Billion in 2006." AMR Research, November 29, 2005.

overall market gains and trailed only slightly the average gain of companies that had no reported problems in 2004 or 2005.[7]

Defining Internal Control

In the preceding sections, we discussed internal control from several points of view. For organizational governance, internal controls (or control activities, or simply controls) are implemented to help ensure that risk responses are effectively carried out, or the controls themselves are the responses to risks. Also, as we have just discussed, internal control is the subject of SOX section 404. But what do we mean by *internal control*? Up to now we have only alluded to this term's meaning. In the next two sections, we describe definitions of internal control found in the authoritative literature and then offer our own working definition.

The COSO Definition of Internal Control

Earlier in this chapter, we introduced *Enterprise Risk Management—Integrated Framework* and the organization that issued that framework, the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In 1992, the COSO organization introduced a framework, *Internal Control—Integrated Framework* that itself became known as "COSO." The definition of internal control contained in COSO has become widely accepted and is the basis for definitions of control adopted for other international control frameworks:[8]

> Internal control is a process—effected by an entity's board of directors, management, and other personnel—designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations[9]

Figure 7.2 depicts the influence that this definition has had on authoritative auditing and control literature. In 1995, Statement on Auditing Standards No. 78 (SAS No. 78), "Consideration of the Internal Control in a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55," adopted the COSO definition of internal control. SAS No. 78, adopting the COSO definition, went on to say that internal control comprises five interrelated components:

- *Control environment:* Sets the tone of an organization, influencing the control consciousness of its people. It serves as the foundation for all other components of internal control by providing discipline and structure.

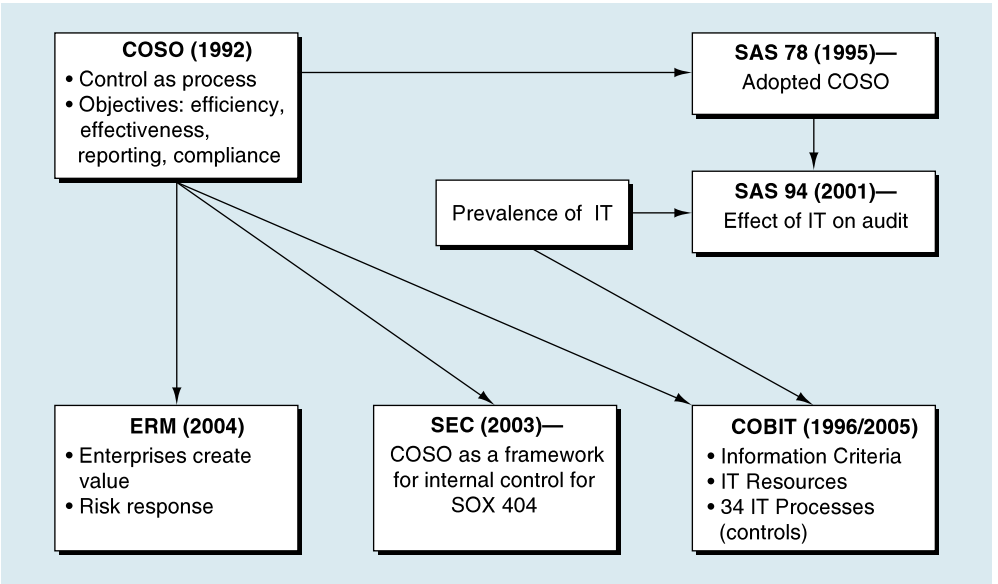
---

7 David Reilly, "Checks on Internal Controls Pays Off." *Wall Street Journal*, May 8, 2006: C3.b n

8 The influence of the COSO definition of internal control is apparent in the definitions adopted by the following: (a) the *Cadbury Report* published as *The Financial Aspects of Corporate Governance* (London: The Committee on the Financial Aspects of Corporate Governance, December 1, 1992); (b) *Preface to Guidance Issued by the Criteria of Control Board* (Toronto, Ontario, Canada: The Canadian Institute of Chartered Accountants, 1995); (c) *COBIT 4.0: Control Objectives for Information and Related Technology* (Rolling Meadows, IL: IT Governance Institute, 2005); and (d) *King Report on Corporate Governance for South Africa 2002* (Parklands South Africa: Institute of Directors in South Africa, 2002).

9 *Internal Control—Integrated Framework—Framework Volume* (New York: The Committee of Sponsoring Organizations of the Treadway Commission, 1992): 9, 12, and 14.

FIGURE 7.2 COSO Influence on Defining Internal Control



- *Risk assessment:* The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.
- *Control activities:* The policies and procedures that help ensure that management directives are carried out.
- *Information and communication:* The identification, capture, and exchange of information in a form and timeframe that enables people to carry out their responsibilities.
- *Monitoring:* A process that assesses the quality of internal control performance over time.

As the influence of IT over information systems, financial reporting, and auditing became clearer, the IT auditing and auditing communities responded. In 1996, the Information Systems Audit & Control Association (ISACA) issued COBIT (Control Objectives for Information and Related Technology) with a definition of internal control that closely paralleled COSO.[10] COBIT's 34 IT processes form the basis of our discussion of pervasive and general controls in Chapter 8. In 2001, the Auditing Standards Board issued Statement on Auditing Standards No. 94 (SAS No. 94), "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit." SAS No. 94 provided guidance on how an organization's IT might affect any of COSO's five components of internal control. This standard guides auditors in understanding the impact of IT on internal control and assessing IT-related control risks.

On June 5, 2003, the SEC issued the final rules related to implementation of SOX, "Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports."[11] In the section addressing

10 COBIT version 4 was released in 2005 by an ISACA sister organization, the IT Governance Institute.

11 SEC Release No. 33-8238, June 5, 2003.

implementation of SOX section 404, the SEC used the COSO description of internal control. It went on to say that management must base its evaluation of the effectiveness of its internal control system on a framework such as COSO. PCAOB Auditing Standard No. 2 uses COSO in its description of the conduct of an integrated audit under SOX 404. Finally, you may have noticed the similarity of the eight components of ERM outlined in Exhibit 7.1 (pg. 209) and the five components of COSO. The ERM framework emphasizes the compatibility of ERM, and COSO and suggests that organizations and auditors should continue to use COSO as a basis for internal control. Armed with this background perspective and the importance of COSO in the definition of internal control, let's now proceed to a working definition of internal control that will be used throughout the remainder of the text.

Working Definition of Internal Control

The common ground on which we have developed our working definition of internal control includes the following points of general agreement:

- Consult the definition of ERM (pg. 208) and COSO's definition of internal control (pg. 216) and notice that both refer to internal control as a process for accomplishing objectives. We introduced several processes in Chapter 1. In general, a **process** is a series of actions or operations leading to a particular and usually desirable result. Results could be risk management as described by ERM, effective internal control as proposed by COSO, or a specified output of an operations process for a particular market or customer.
- Internal control might also be referred to as a system. Consistent with the definition of system in Chapter 1, internal control (1) has clearly defined objectives and (2) consists of interrelated components that act in concert to achieve those objectives.
- As noted in Title IV of SOX (see Exhibit 7.4 on pgs. 214–215), establishing and maintaining a viable internal control system is *management's* responsibility. In fact, ultimate ownership of the system should rest with the CEO. Only if the primary responsibility for the system resides at the top can control effectively permeate the entire organization.
- The strength of any internal control system is largely a function of the people who operate it. In other words, no matter how sound the control *processes* may be, they will fail unless the personnel who apply them are competent and honest. Because internal control is so people-dependent, we explore the ethical dimensions of control more fully later in the chapter.
- Partly because it depends on people to operate it and partly because it comes only at some cost to the organization, internal control cannot be expected to provide *absolute*, 100 percent assurance that the organization will reach its objectives. Rather, the operative phrase is that it should provide *reasonable assurance* to that effect.
- Internal control is not free; it has a cost associated with it. For that reason, it should result from management's thoughtful risk analysis and evaluation of costs and benefits. Controls should be "built in versus bolted on." That is, to be cost-effective, controls should not be superimposed on the existing organizational structure. Rather, they should be purposefully designed and integrated with existing operational activities. As the COSO report expressed it:

> The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are part of the essence of the enterprise.

"Built-in" controls support quality and empowerment initiatives, avoid unnecessary costs, and enable quick response to changing conditions.[12]

Given the prominence of COSO in developing these ideas and in defining internal control, we offer the following definition of control (as also defined in the Preface and Chapter 1), which will be used to guide our study of the topic throughout the remainder of the text:

Internal control is a process—effected by an entity's board of directors, management, and other personnel—designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

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

The only modification that we make to the COSO definition is to broaden our scope beyond financial reporting to include all reporting. This definition is more expansive than the scope of internal controls subject to reviews under SOX 404, because we include efficiency and effectiveness of operations and all reporting, not just financial reporting.

Let's put a few things together at this point and see what we have learned. Organizational governance, as implemented with a framework such as ERM, begins with establishing mission, vision, and purpose; then, strategy and objectives directed at the mission are established (see Figure 7.1 on pg. 208). Next, events that could affect achieving objectives, including opportunities and risks, are identified. After assessing risks and deciding how to respond to the risks, controls are put in place to ensure that responses to the risks are carried out. COSO and our own definition of internal control jump in at this point by describing internal control as a process for achieving objectives. We conclude then by saying that the purpose of internal control is to provide reasonable assurance that objectives are achieved and that risk responses are carried out.

How do we determine whether a system of internal control is designed well and can help an organization achieve objectives and respond to risks? Typically, a key tool in the assessment of a system of internal control is a *matrix* such as that depicted in Figure 7.3.

FIGURE 7.3 Matrix for Evaluating Internal Controls

	Objectives				
Processes (with controls)	Strategy setting	Effectiveness of operations	Efficiency of operations	Reliability of reporting	Compliance with laws and regulations
Process 1	✓			✓	
Process 2		✓			✓
Process 3		✓	✓	✓	
Process n	✓				✓

12 *Internal Control—Integrated Framework—Executive Summary Volume* (New York: The Committee of Sponsoring Organizations of the Treadway Commission, 1992): 3.

Technology Summary 7.1

2006 REPORT TO THE NATION ON OCCUPATIONAL FRAUD AND ABUSE

Between January 2004 and January 2006, the Association of Certified Fraud Examiners gathered information from Certified Fraud Examiners (CFEs) throughout the United States about fraud cases that they had personally investigated. The median loss of the 1,134 cases of fraud reported by the CFEs was $159,000. Nearly one-quarter of these cases caused at least $1 million in losses, and 9 cases resulted in losses of greater than $1 billion dollars. In the report summarizing these frauds, we learn the following:

- Respondents estimated that the typical U.S. organization loses 5 percent of annual revenues to fraud, which if projected to the entire economy, would total $652 billion in total losses.
- The median time that the frauds were underway before being detected was 18 months.
- Frauds were more likely to be detected by tips (e.g., through hotlines such as those required by SOX) than through audits or internal controls.
- Median losses were twice as high in organizations without hotlines.
- Small businesses—those with fewer than 100 employees—suffer disproportionately larger losses and are more vulnerable because they are least likely to have a hotline, an internal audit department, surprise audits, and fraud training.
- Small business frauds involved employees fraudulently writing company checks, skimming revenues, and processing fraudulent invoices.
- Fraud losses caused by owners and executives were five times higher than those caused by managers and 13 times higher than those caused by employees.
- Frauds were committed by employees in the accounting department (30 percent of frauds) and upper management (20 percent of frauds).

Source: *2006 ACFE Report to the Nation on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2006).

Figure 1.7 in Chapter 1 (pg. 22) depicted a similar matrix for assessing achievement of qualities of information such as timeliness (i.e., effectiveness), validity, accuracy, and completeness (i.e., reliability of reporting). The concept here is the same and will be repeated several times in this text. Figure 7.3 shows that we have established five high-level categories of objectives. And, we have listed a sample of the processes/controls that address these objectives (from the definition of ERM). The check marks show which processes address which objectives. You can see, for example, that processes 2 and 3 are directed at effectiveness of operations. If you go back to the example in Figure 7.1 (pg. 208), this objective might be to increase production of product x by 15 percent.

If we stop with the *design* of the system of internal control, we use this matrix to simply ask the question, "can these processes/controls provide reasonable assurance that the objectives are achieved?" In this example, we would ask if these processes and controls can provide reasonable assurance that production can be increased by 15 percent.

The assessment concludes with recommendations for changes to the processes and controls that might be necessary. Such recommendations must be made very carefully, as there are many cost-benefit factors to consider. Changes can include changes to process activities (i.e., purchasing raw materials) or changes to process controls (i.e., approving purchase orders). If changes in the process do not reduce the variance from objectives, changes to process objectives (e.g., increase production by only 5 percent) might also be considered.

Because control is an ongoing process, there are periodic iterations of the steps just outlined. For example, as we will discuss next with regard to fraud, periodic reviews are conducted to determine the effectiveness of fraud-prevention programs.

TECHNOLOGY SUMMARY 7.2

GLOBAL ECONOMIC CRIME SURVEY 2005

In 2005, PricewaterhouseCoopers conducted its third, biennial Economic Crime Survey. Key findings, based on interviews with more than 3,600 senior executives in 34 countries, include the following:

- 45 percent of companies reported frauds in the past two years, an 8 percent increase over the 2003 survey.
- Larger companies reported more incidents of fraud than the average (12 vs. 8 average reported incidents).
- Since the 2003 survey, the number of companies reporting corruption and bribery increased 71 percent, the number reporting money laundering increased 133 percent, and the number reporting financial misrepresentation increased 140 percent.
- Asset losses due to frauds caused average losses of $1.7 million, a 50 percent increase over 2003.
- Most frauds (34 percent) were detected by chance. But, companies with fraud-detection measures uncover more frauds than do companies that rely on internal controls and audits to detect fraud.

Source: PricewaterhouseCoopers *Global Economic Crime Survey 2005*, 2005.

Fraud and Its Relationship to Control

In this section, we discuss fraud, computer fraud, and computer abuse and emphasize that an organization's system of internal control must be designed to address the risks of fraud. **Fraud** is a deliberate act or untruth intended to obtain unfair or unlawful gain. Management's legal responsibility to prevent fraud and other irregularities is implied by laws such as the Foreign Corrupt Practices Act,[13] which states that "a fundamental aspect of management's stewardship responsibility is to provide shareholders with reasonable assurance that the business is adequately controlled." Notice that Title XI of the Sarbanes-Oxley Act specifically addresses corporate fraud.

The accounting profession has been proactive in dealing with corporate fraud. For example, one outcome of an antifraud program is Statement on Auditing Standards No. 99 (SAS No. 99), "Consideration of Fraud in a Financial Statement Audit." SAS No. 99 emphasizes brainstorming fraud risks, increasing professional skepticism, using unpredictable audit test patterns, and detecting management override of internal controls. Paragraph 26 of PCAOB Auditing Standard No. 2 (AS2) describes management's responsibility to design an organization's internal control system to "prevent, deter, and detect fraud." AS2 paragraph 24 requires that auditors "evaluate all controls specifically intended to address risks of fraud."

Why are Congress, the accounting profession, the financial community, and others so impassioned about the subject of fraud? This is largely because of some highly publicized business failures in recent years that caught people completely by surprise because the financial statements of these businesses showed that they were prospering. When these firms, such as Enron, went "belly-up," it was discovered that the seeming prosperity was an illusion concocted by "cooking the books" (i.e., creating false and misleading financial statements).

Aside from some widely reported cases, is fraud really that prevalent in business? First, Technology Summary 7.1 describes the highlights of a report issued by the Association of Certified Fraud Examiners. Notice the total estimated fraud losses and the disproportionate number of frauds committed against small businesses. Second, Technology Summary 7.2 describes the results of the 2005 Global Economic Crime Survey conducted by PricewaterhouseCoopers (PwC).

13 See the Foreign Corrupt Practices Act (FCPA) of 1977 (P.L. 95-213).

We can see from the PwC report that fraud is indeed a worldwide problem and that it is increasing. We can see from both reports that the losses are significant. Because of the survey population, we get differing findings on the impact on smaller organizations. However, both reports agree that internal controls and audits are not sufficient to detect fraud. Fraud-prevention programs and detection measures, such as hotlines, are necessary to address the risk of fraud. The implication is clear: a system of internal control, including an ongoing *process* of review, can reduce the incidents of fraud.

Implications of Computer Fraud and Abuse

E-BUSINESS

Now let's turn our attention to computer fraud and abuse. The proliferation of computers in business organizations has created expanded opportunities for criminal infiltration. Computers have been used to commit a wide variety of crimes, including fraud, larceny, and embezzlement. In general, computer-related crimes have been referred to as *computer fraud*, *computer abuse*, or *computer crime*. Some of these frauds are more prevalent when an organization is engaged in e-business. For example, an organization that receives payment via credit card, where the credit card is not present during the transaction (e.g., sales via Web site or telephone), absorbs the loss if a transaction is fraudulent. To prevent these losses, the organization may install controls, such as antifraud software. Also, some banks will drop merchants who have unacceptably high fraud rates. This would cause an organization to go out of business. In addition, an organization must undertake measures to prevent losses to its customers that may come about from such fraudulent activities as *spybots* and *keyloggers*. Let's now examine some of these fraud techniques and the means for coping with them.

Computer crime includes crime in which the computer is the target of the crime or the means used to commit the crime.[14] The majority of computer crimes fall into these two basic types:

- The computer is used as the *tool* of the criminal to accomplish the illegal act. For instance, the perpetrator could illegally access one or more banking systems to make unauthorized transfers to a foreign bank account and then go to the other country to enjoy the ill-gotten gain.
- The computer or the information stored in it is the *target* of the criminal. *Computer viruses* fall into this category.

E-BUSINESS

Technology Summary 7.3 provides a brief presentation of computer viruses, a general category of computer abuse that includes the more specific examples of malicious coding techniques described in Technology Summary 7.4 (pg. 224). *Computer hacking*, another category of computer abuse is discussed in Chapter 8. All of these techniques are major concerns to organizations engaged in e-business because they affect the actual and perceived reliability and integrity of their electronic infrastructure. Be aware of two things: insiders commit the majority of computer crimes, and the methods listed are by no means exhaustive.

Before leaving this section, let's make a few other points. First, systems have been manipulated in a number of different ways in perpetrating computer crimes. Manipulation of event-related data (i.e., the adding, altering, or deleting of events) represents one frequently employed method of committing computer fraud.

Second, regardless of the method used in committing computer crime, we must not overlook the real issue. Computer crime represents an interesting example of a process

14 We use the terms *computer crime*, *computer abuse*, and *computer fraud* interchangeably. Technically, they refer to slightly different concepts, but we do not need to distinguish between them for your discussions here.

Technology Summary 7.3

COMPUTER VIRUSES

A **computer virus** is program code that can attach itself to other programs (including macros within word processing documents), thereby "infecting" those programs and macros. Viruses can *reproduce themselves* in a manner analogous to biological viruses. Viruses are activated when you run an infected program, open an infected document, or boot a computer from an infected disk. Computer viruses alter their "host" programs, destroy data, or render computer resources (e.g., disk drives, central processor, networks) unavailable for use.

Some viruses are fairly innocent—they might merely produce a message such as "GOTCHA" or play "The Blue Danube" through the computer's speakers. Other viruses can be more harmful. Some viruses will delete programs and files; some will even format your hard drive, thus wiping away all stored data! Viruses also can overload local area networks with "messages," making it impossible to send or receive e-mail or to connect to external sources, such as the Internet. Finally, denial-of-service attacks, where hackers continuously deluge Web servers with high volumes of messages (called mass mailers) can render a server so busy handling the onslaught of messages that legitimate customers are prohibited from gaining access and conducting business with the companies.

Viruses can enter an organization through software that is shared through the exchange of storage media (i.e., peer-to-peer technologies), Web server vulnerabilities, and e-mail. Such exchanges allow viruses to quickly become an epidemic, much like a biological virus. The real fear that can cause information systems managers to lose sleep, of course, is that the virus will then spread to the organization's networks (and networked computing resources) and destroy the organization's most sensitive data or result in denial of service to customers.

How extensive is the virus problem? In its 2004 "10th Annual ICSA Labs Virus Prevalence Survey,"[a] ICSA Labs®, an independent division of Cybertrust, Inc.®, reported 392 monthly virus infection encounters per 1,000 PCs in 2004, up by nearly 50 percent from 2003. The number of virus disasters—25 or more computers infected at the same time by the same virus—was up 12 percent from 2003. The average number of days to recover was 7 person-days and cost $130,000, both increases of over 25 percent from 2003.

How do you protect your computer from a viral infection? The ICSA report suggests that typical defensive technologies, such as antivirus software and firewalls, should be used in combination with personnel policies, practices, and training, file attachment filtering, and so on.

[a] Cybertrust, Inc.®, ICSA Labs 10th Annual ICSA Labs Virus Prevalence Survey, 2004.

failure. It characterizes a poorly controlled process. Process failure can usually be corrected by a conscientious application of appropriate control plans. For example, inadequately controlled changes to programs (see *program change* controls in Chapter 8) have allowed programmers to insert malicious code such as Trojan Horses and Logic Bombs into legitimate programs to perpetrate major frauds. If access to the computer programs and data are protected, frauds can be prevented.

Finally, as seductive as the topic of computer fraud and abuse is for students, you should not leave this section with the mistaken impression that controls are important simply because they can protect against "rip-offs." It has been estimated that losses due to accidental, nonmalicious acts far exceed those caused by willful, intentional misdeeds. Therefore, you should recognize that the computer must be protected by a system of controls capable not only of preventing crimes but also of minimizing simple, innocent errors and omissions.

Technology Summary 7.4

MALICIOUS CODE TECHNOLOGIES

- *Salami slicing:* Unauthorized instructions are inserted into a program to systematically steal very small amounts, usually by rounding to the nearest cent in financial transactions such as the calculation of interest on savings accounts. A dishonest programmer includes an instruction that if the amount of interest to be credited to the account is other than an even penny (for example, $2.7345), the excess over the even amount (.0045) is to be credited to account number 673492, which just happens to be his own. Although each credit to his account is minute, the total can accumulate very rapidly.
- *Back door:* During the development of a program, the programmer may insert a special code or password that enables him to bypass the security features of the program to access the program for troubleshooting or other purposes. These are meant to be removed when the programmer's work is done, but sometimes they aren't and can be used by others to attack the program.
- *Trojan Horse:* A module of unauthorized computer code is covertly placed in a seemingly harmless program. The program executes its intended function, while the malicious code performs an unauthorized act such as destroying your hard disk. Trojan Horses are often distributed via e-mail as a *computer virus*. Trojan Horses, such as *spybots* that report on Web sites that a user visits, and *keyloggers* that log keystrokes and send the information back to clients, can be inadvertently downloaded by visiting the wrong Web site or clicking on the wrong hyperlink.
- *Logic Bomb:* Code, secretly inserted into a program, is designed to execute (or "explode") when, for example, a specific date or event occurs (i.e., a delayed-action *Trojan Horse* or *computer virus*). The code may display a harmless message, or it could cause a disaster, such as shutting a system down or destroying data.
- *Worm:* This type of *computer virus* replicates itself on disks, in memory, and across networks. It uses computing resources to the point of denying access to these resources to others, thus effectively shutting down the system.
- *Zombie (zombie agent, zombie network):* This program secretly takes over another Internet-attached computer and then uses that computer to launch attacks that can't be traced to the zombie's creator. Zombies are elements of the denial-of-service attacks discussed in Chapter 8.

Ethical Considerations and the Control Environment

Before discussing our framework for analyzing a system of internal control, let's pause to examine the very underpinnings of the system—namely, its ethical foundation. COSO places integrity and ethical values at the heart of what it calls the *control environment* (captured in ERM as *internal environment*). In arguing the importance of integrity and ethics, these frameworks make the case that the best designed control systems are subject to failure caused by human error, faulty judgment, circumvention through collusion, and management override of the system. COSO, for example, states that:

> Ethical behavior and management integrity are products of the "corporate culture." Corporate culture includes ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. Official policies specify what management wants to happen. Corporate culture determines what actually happens and which rules are obeyed, bent, or ignored.[15]

15 *Internal Control—Integrated Framework—Framework Volume* (New York: The Committee of Sponsoring Organizations of the Treadway Commission, 1992): 20.

There is some evidence to suggest that companies with formal ethics policies might even lower their internal control costs. Cases in point: the business and audit failures noted at the beginning of this chapter arose primarily because upper management did not establish and/or reinforce ethical corporate cultures across their organizations; in some cases, managers willfully violated any semblance of ethical behavior.

Management is responsible for internal control and can respond to this requirement legalistically or by creating a control environment. That is, management can follow the "letter of the law" (its form), or it can respond *substantively* to the need for control (its spirit). The **control environment** reflects the organization's (primarily the board of directors' and management's) general awareness of and commitment to the importance of control throughout the organization. In other words, by setting the example and by addressing the need for control in a positive manner at the top of the organization, management can make an organization *control conscious*.

For instance, reward systems might consider ethical, legal, and social performance, as well as the "bottom line."[16] Imagine the temptation to circumvent the control system or to "bend the rules" that could result from a reward system that pressures employees to meet unrealistic performance targets—such as happened at Enron Corporation—or that places upper and lower limits on employee bonus plans. Strategies should be developed that do not create conflicts between business performance and legal requirements. Finally, management should consistently find it unacceptable for personnel to circumvent the organization's system of controls, and, as importantly, the organization *should impose stiff sanctions for such unacceptable behavior*. These actions are included in what some call the "tone at the top" of the organization.

Aside from the companies mentioned in the introduction to this chapter, there are numerous examples of frauds and other illegal acts perpetrated by upper management. For example, at DaimlerChrysler AG's Mercedes unit, there were accusations that bribes were paid in at least a dozen countries,[17] and that senior executives may have been aware of the practice. The inquiry stemmed from a wrongful-dismissal lawsuit in which a former Chrysler accountant alleged that he was fired in part because he complained to superiors about secret bank accounts being kept by the Mercedes unit.[18] An organization's board of directors, audit committee, and internal and external auditors must always be alert to the possibility that the "tone at the top" has become as distorted as indicated in this case.

One tangible way an increasing number of companies have articulated the ethical behavior expected of employees is to develop corporate *codes of conduct* that are periodically acknowledged (i.e., signed) by employees. The codes often address such matters as illegal or improper payments; conflicts of interest; insider trading; computer ethics, including personal use of office e-mail systems and Internet connections; and software piracy.

---

16 COSO even goes as far as to suggest that responsibility for internal control should be an explicit or implicit part of everyone's job description.

17 Bribes by companies or individuals were outlawed by the U.S Foreign Corrupt Practices Act of 1977 (P.L. 95-213) and in the European Union by the Organization of Economic Cooperation and Development (OECD) Anti-Bribery Convention of 1997.

18 John R. Wilke and Stephen Power, "U.S. Probes Allegations of Bribery at DaimlerChrysler; Launch of Criminal Inquiry Stems from Lawsuit Claims of Illegal Foreign Payouts," *Wall Street Journal* (August 5, 2005): A1, A6.

A Framework for Assessing the Design of a System of Internal Control

In this final major section of this chapter, we begin our presentation of a framework for assessing the design of a system of internal control, including defining control goals and controls plans. We continue to employ a matrix to assist us in our analysis. We call this particular type of matrix a **control matrix**, which is a tool designed to assist you in evaluating the potential effectiveness of controls in a business process by matching control goals with relevant control plans. To focus our discussion throughout the rest of the chapter, we will apply control concepts to the Lenox Company cash receipts process depicted in Figure 7.4. The associated narrative is included in Exhibit 7.5 (pg. 228). Before proceeding, be sure to acquaint yourself with the figure and exhibit.

As a manager, what are your concerns about this process? That is, what are your objectives and the related risks? Let's review a few concerns:

- We want all of the checks to be deposited in a timely manner, but checks might be lost, stolen, or delayed.
- We want of the deposits to be recorded correctly, but we might miss some checks, record checks we don't have, or record the check amounts incorrectly.
- We want all customer payments to be recorded correctly (i.e., correct account and amount).
- We want to accomplish all this with a minimum of resources such as the clerks and the computer in Figure 7.4.

A recurring theme throughout this text has been that an organization defines objectives, assesses risks, and then establishes processes and controls to provide reasonable assurance that those objectives are achieved (and that there is an appropriate response to the risks). Refer, for example, to Figure 1.7 in Chapter 1 (pg. 22), Exhibit 7.3 (pg. 212), and Figure 7.3 (pg. 219). The purpose of internal control as defined in this text is consistent with that theme. The purpose is to provide reasonable assurance of achieving objectives in three categories: *operations* (efficient and effective), *reporting* (i.e., reliable), and *compliance* with applicable laws and regulations. For our control framework, we convert those three categories into control goals for two categories, *operations process control goals* (for efficiency and effectiveness) and *information process control goals* (for reliable reporting).[19] Notice that these two categories correspond to operations and management processes in Figure 1.4 (pg. 15).[20] **Control goals** are business process objectives that an internal control system is designed to achieve. Figure 7.5 (pg. 229) depicts the breakdown of these goals as column headings on a portion of our control matrix. Table 7.1 (pg. 230) provides an overview of the *generic* control goals of the *operations process* and *information process*. In the following paragraphs, we discuss each goal, and ask you to follow Figure 7.5, Table 7.1, and Figure 7.4 in the process.

19 We include *compliance with applicable laws, regulations, and contractual agreements* as one of the goals of each *operations process* to which such laws, regulations, or agreements might be appropriate. For instance, compliance with the Robinson/Patman Act is shown as a legitimate goal of the order entry/sales system process in Chapter 10.

20 For simplicity, our analysis of controls does not include the third business process component, the management process.

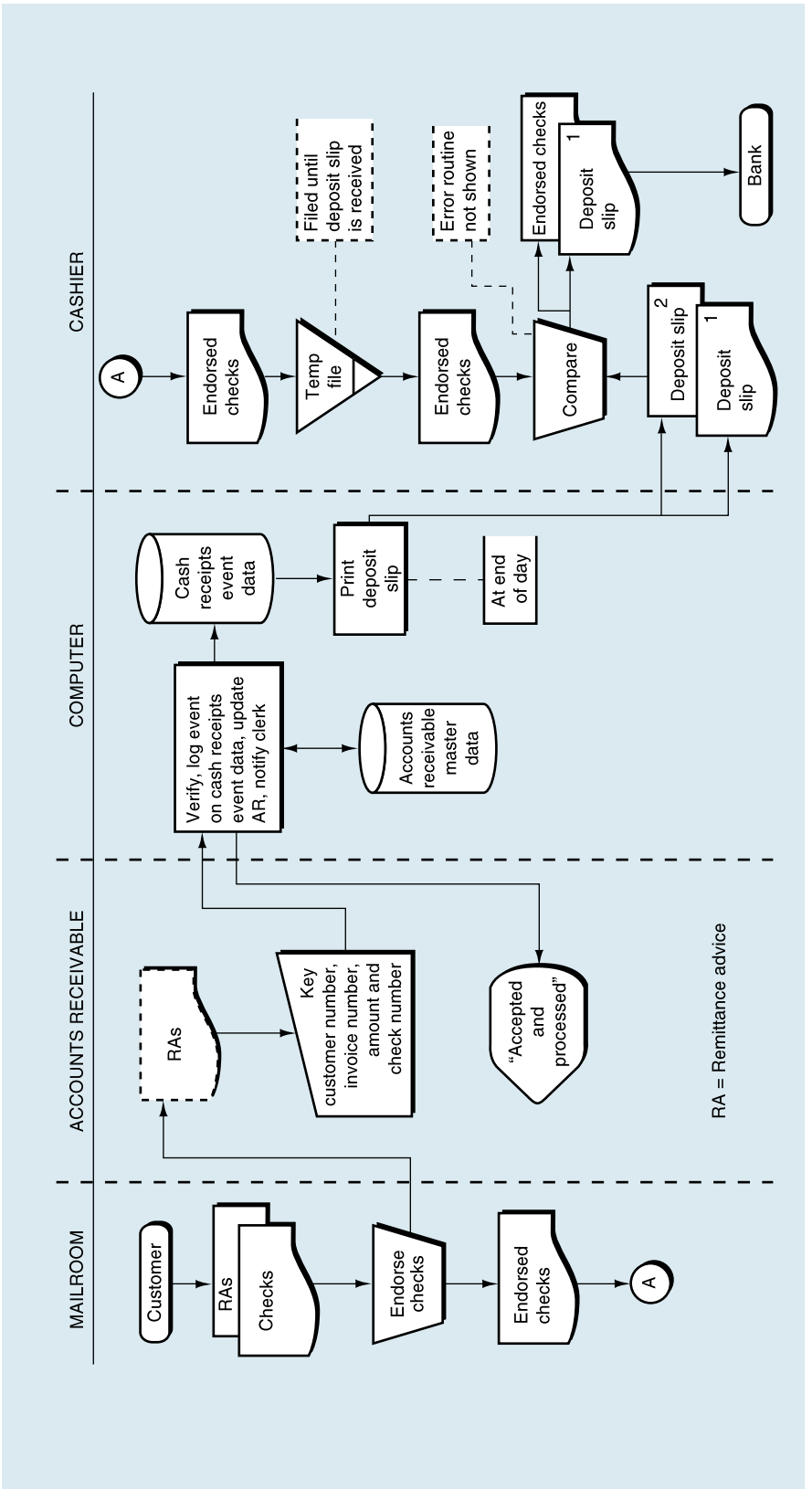


FIGURE 7.4 Lenox Company Systems Flowchart

EXHIBIT 7.5 Lenox Company System Narrative

The Lenox Company uses the following procedures to process the cash received from credit sales. Customers send checks and remittance advices (i.e., the stubs from the bills received from Lenox) to the Lenox mailroom where clerks endorse the checks and send the remittance advices to accounts receivable and the checks to the cashier.

In accounts receivable, a clerk enters the RAs into the computer by keying the customer number, invoice number, amount paid, and the check number. After verifying that the invoice is open and that the correct amount is being paid, the computer logs the payment data on the cash receipts event data store, updates the accounts receivable master data to reflect the payment, and notifies the clerk that the input has been accepted and that the accounts receivable master data has been updated.

At the end of each day, the computer uses the payment data on the cash receipts event data store to print deposit slips in duplicate on the printer in the cashier's office. The cashier compares the deposit slips to the corresponding checks and then takes the deposit to the bank.

Control Goals of Operations Processes

The first control goal, *ensure effectiveness of operations*, strives to ensure that a given operational process (e.g., Lenox's cash receipts process) is fulfilling the purpose for which it was intended. Notice that we must itemize the specific *effectiveness (i.e., operations process) goals* to be achieved. In Figure 7.5, we show two examples (i.e., timely deposit and comply with compensating balance agreement). These goals are created by people and are therefore subjective, so no uniform set of process goals exists. In each of the business process chapters, we provide a representative listing of effectiveness goals.

The next goal, *ensure efficient employment of resources*, can be evaluated in only a relative sense. For example, to determine efficiency in achieving Lenox's effectiveness goal to deposit checks in a timely manner, we would need to know the cost of the people and computer equipment required to accomplish this goal. If the cost is more than the benefits obtained (e.g., security of the cash, interest earned), the system might be considered *in*efficient. Likewise, if the Lenox process costs more to operate than a process in a similar organization, we might also judge the system to be *in*efficient.

Let's now discuss the last operations process control goal in Table 7.1: to *ensure security of resources*. As noted in the table, organizational resources take many forms, both physical and nonphysical. Since the advent and proliferation of computer systems, information has become an increasingly important resource. For example, the information about Lenox's accounts receivable data represents an important resource for this company. Without the data, it would be virtually impossible to collect these receivables. Lenox must protect all of its resources, both tangible and intangible.

Control Goals of Information Processes

A glance at Table 7.1 (pg. 230) and Figure 7.5 reveals that the first three control goals related to the information process deal with entering event-related data into a system. Recall from Chapter 1 that data input includes *capturing* data (for example, completing a source document such as a sales order). Also, data input includes, if necessary, *converting* the data to *machine-readable form* (for example, for Lenox, keying the remittance advices). Therefore, *event data* are the targets of the *input* control goals shown in Table 7.1 and Figure 7.5.

FIGURE 7.5 Control Goals for the Lenox Cash Receipts Process

Control Goals of the Lenox Cash Receipts Business Process								
Control Goals of the Operations Process				Control Goals of the Information Process				
Ensure effectiveness of operations		Ensure efficient employment of resources (e.g., people and computers)	Ensure security of resources (e.g., checks and AR master data)	For the remittance advice inputs, ensure:			For the AR master data, ensure:	
A	B			IV	IC	IA	UC	UA

Effectiveness goals include:

A – Timely deposit of checks

B – Comply with compensating balance agreements with the depository bank

IV = Input validity

IC = Input completeness

IA = Input accuracy

UC = Update completeness

UA = Update accuracy

To illustrate the importance of achieving the first goal, *ensure input validity*, assume that Lenox's accounts receivable clerk processes 50 remittance advices (RAs). Further assume that 2 of the 50 RAs represent fictitious cash receipts (for example, a mailroom employee fabricates the phony remittance advices for relatives who are Lenox customers). What is the effect of processing the 50 RAs, including the 2 fictitious remittances? First, the cash receipts event data and the accounts receivable master data have been corrupted by the addition of two bogus RAs. Second, if not detected and corrected, the pollution of these data will result in unreliable financial statements—overstated cash and understated accounts receivable—and other erroneous system outputs (e.g., cash receipts listings, customer monthly statements).

To discuss the second information process goal, *ensure input completeness*, let's return to the previous Lenox example and suppose that, while the 48 *valid* RAs are being key-entered (we'll ignore the 2 fictitious receipts in this example), the accounts receivable clerk decides to get a cup of coffee. As the clerk walks past the batch of 48 RAs, 10 are blown to the floor and are not entered into the system. What is the effect of processing 38 RAs, rather than the original 48? First, the cash receipts event data and the accounts receivable master data will be incomplete; that is, it will fail to reflect the true number of remittance events. Second, the incompleteness of the data will cause the resulting financial statements and other reports to be inaccurate (i.e., understated cash balance and overstated accounts receivable). In this example, the omission was unintentional. Fraudulent, intentional misstatements of the accounting data can be accomplished by omitting some events.

The goal of *input completeness* is concerned with the actual number of events or objects to be processed. Particular questions relative to this goal include the following:

- Is *every* event or object captured (for example, are source documents prepared for every valid event or object)?

TABLE 7.1 Control Goals

Control Goal	Definitions	Discussion
Control Goals of Operations Processes		
Ensure *effectiveness of operations* by achieving selected *goals* for the operations process.	**Effectiveness:** A measure of success in meeting one or more *goals* for the *operations process.*	If we assume that one of Lenox's goals is to deposit checks in a timely manner, the operations process is effective if cash receipts are deposited each day when received.
Ensure *efficient employment of resources* (e.g., people, computers).	**Efficiency:** A measure of the productivity of the resources applied to achieve a set of goals.	The cost of the people, computers, and other resources needed to deposit all checks on the day received.
Ensure *security of resources* (e.g., cash, data assets, inventory)	**Security of resources:** Protecting an organization's resources from loss, destruction, disclosure, copying, sale, or other misuse.	Physical (e.g., cash) and nonphysical (e.g., information) resources are available when required and put only to authorized use.
Control Goals of Information Processes		
Ensure *input validity* (IV).	**Input validity:** Input data are appropriately approved and represent actual economic events and objects.	Only cash receipts supported by actual checks should be input into the Lenox process.
Ensure *input completeness* (IC).	**Input completeness:** All valid events or objects are captured and entered into a system.	All valid customer payments are entered into the Lenox process.
Ensure *input accuracy* (IA).	**Input accuracy:** All valid events must be correctly captured and entered into a system.	The customer, invoice, check numbers, and amount of payment must be keyed correctly into the Lenox computer.
Ensure *update completeness* (UC).	**Update completeness:** All events entered into a system must be reflected in the respective master data.	All cash receipts entered must be recorded on the accounts receivable master data.
Ensure *update accuracy* (UA).	**Update accuracy:** Data entered into a system must be reflected correctly in the respective master data.	All cash receipts entered must be correctly recorded in the accounts receivable master data.

- Is every captured event or object *entered into the computer* (or manually recorded in the books of original entry)? This was the breakdown in the Lenox example of 10 RAs getting blown to the floor and overlooked.

When dealing with input completeness, we are concerned with the documents or records representing an event or object, not the *correctness* or *accuracy* of the document or record. Accuracy issues are addressed by the third information process goal. Input completeness simply means that *all* of the events or objects that should be processed (i.e., the valid events and objects) are processed.

The third information process goal, *ensure input accuracy*, relates to the various data items that usually constitute a record of an event, such as a source document. To achieve this goal, we must minimize discrepancies between data items entered into a system and the economic events or objects they represent. Mathematical mistakes and inaccurate transcription of data from one document or medium to another may cause accuracy errors. Again, let's return to the Lenox example. Suppose that one of the *valid* RAs is from Acme Company, customer 159, in the amount of $125. The accounts receivable clerk mistakenly enters the customer number as 195, resulting in Ajax Inc.'s account

(rather than Acme's) being credited with the $125. Missing data fields on a source document or computer screen represent another type of accuracy error. For Lenox, the absence of a customer number on a remittance advice would result in "unapplied" cash receipts (that is, receipts that can't be credited to a particular customer). We consider this type of system malfunction to be an accuracy error rather than a completeness error because the mere presence of the source document suggests that the event itself has been captured and that the input data are, by our definition, therefore complete.

Two critical questions must be asked concerning the goal of input accuracy:

- Is the initial capturing of data correct (for example, are data recorded accurately on source documents)?
- Is the entered data correct (for example, are data transcribed or recorded in the books of original entry or correctly converted from source documents into machine-readable form)? Again, the Lenox example of keying an incorrect customer number was an inaccurate input.

To achieve the goal of input accuracy, we must capture and enter into a system all important data elements. Thus, all important data elements must be identified for each economic event or object that we want to include in a system's database. In general, you should find the following guidelines helpful in identifying important data elements:

- All financial data elements are usually important, such as numbers that enter into a calculation. For a Lenox cash receipt, the gross invoice amount, discount taken, and net amount collected are crucial to "balancing" each RA.
- Reference numbers, such as those for inventory items, customer numbers, and general ledger coding, are important. Among other reasons, accurate reference numbers are crucial to the proper *classification* of items in the financial statements.
- Dates are also very important so that we can determine that events are recorded in the proper time period. For instance, if cash received by Lenox on December 29th was recorded as received on December 28th, would you as an auditor be concerned? Possibly, but not nearly as concerned as you would be if cash received on January 2nd was recorded as received on December 31st (assuming that Lenox's year-end is December 31st). Notice that this accuracy error causes cash receipts to be invalid in December (the cash was not received in December) and incomplete in January (a cash receipt that occurred in January has not been recorded in January).

Now let's examine the last two information process control goals shown in Table 7.1 and Figure 7.5 (pgs. 230 and 229). These goals deal with updating *master data*. As you learned in Chapter 3, master data update is an information-processing activity whose function is to incorporate new data into existing master data. You also learned that there are two types of updates that can be made to master data: *information processing* and *data maintenance*. You also should remember from Chapter 3 that master data updates resulting from information processing are analogous to the *posting* step in a manual bookkeeping cycle. In this textbook, we emphasize information processing; therefore, our analysis of the internal controls related to data updates is restricted to data updates from information processing.

In a manual-based system, the goals of *ensure update completeness* and *ensure update accuracy* relate to updating various ledgers (for example, the accounts receivable subsidiary ledger) for data items entered into the books of original entry (e.g., the sales and cash receipts journals). In Lenox's process, the goal of *ensure update completeness* relates to crediting customer balances in the accounts receivable master data for *all* cash collections recorded in the cash receipts event data. The goal of *ensure update accuracy* relates

to correctly crediting (e.g., correct customer, correct amount) customer balances in the accounts receivable master data.

After valid data have been *completely* and *accurately* entered into a computer (i.e., added to event data such as Lenox's cash receipts event data), the data usually go through a series of processing steps. Several things can go wrong with the data after they have been entered into a computer for processing. Accordingly, the goals of update completeness and accuracy are aimed at minimizing processing errors.

In general, an awareness of the following types of processing errors should assist you in achieving the goals of update completeness and update accuracy:

- *Programming errors:* For example, logical or technical errors may exist in the program software. (For instance, instead of crediting Lenox's customers for cash collections, the cash receipts were *added* to accounts receivable balances.)
- *Operational errors:* For example, today's cash receipts data may be processed against an out-of-date (yesterday's) accounts receivable master data. Or we may fail to execute some intermediate steps in a process. This may happen if input data is used for more than one application, and we fail to use the inputs for all of the intended processes. (Note that this should not be a problem with enterprise systems where one input automatically impacts all relevant applications.) Finally, some applications (such as in banking) process "memo" updates during the day to immediately reflect activity, such as cash withdrawals. The "real" updates take place overnight in a batch process. If we fail to properly execute the overnight process, the updates may be incomplete or inaccurate.

ENTERPRISE SYSTEMS

These two examples present illustrations of how things can go wrong while updating master data, even when the data are valid, complete, and accurate at the input stage. Controls that ensure *input* accuracy and completeness do not necessarily ensure *update* accuracy and completeness. We should note, however, that if the events or transactions are processed using an *online real-time (OLRT) processing* system such as the one depicted in Figure 3.3 (pg. 71 in Chapter 3), the input and update will occur nearly simultaneously. This will minimize the possibility that the update will be incomplete or inaccurate. This is the case with the Lenox process where the input to the cash receipts event data store occurs simultaneously with the update to the accounts receivable master data.

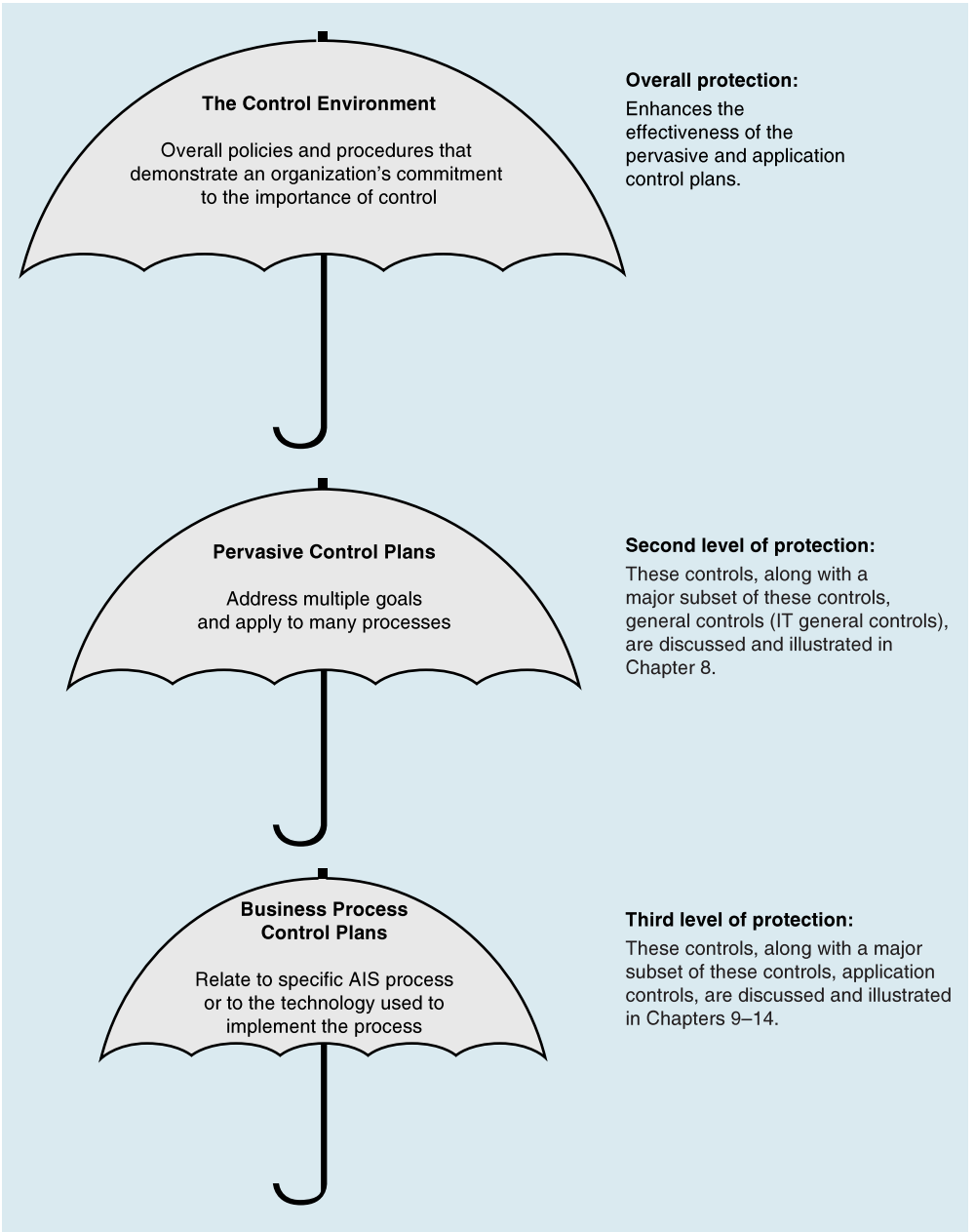
Note that we do *not* have a separate goal for *update validity* as we do for update completeness and update accuracy. The reason is that there is no inherent risk of having an invalid update to master data unless an invalid input data has been introduced into the system. Therefore, by controlling *input* validity, we automatically facilitate update validity.

Control Plans

Control plans reflect information-processing policies and procedures that assist in accomplishing control goals. Control plans can be classified in a number of different ways that help us to understand them. Figure 7.6 shows one such classification scheme. The fact that the *control environment* appears at the top of the hierarchy illustrates that it comprises a multitude of factors that can either reinforce or mitigate the effectiveness of the pervasive and application control plans.

The second level in the Figure 7.6 control hierarchy consists of pervasive control plans. **Pervasive control plans** relate to a multitude of goals and processes. Like the control environment, they provide a climate or set of surrounding conditions in which the various business processes operate. They are broad in scope and apply equally to all business processes; hence, they *pervade* all systems. **General controls**—also known as

FIGURE 7.6 A Control Hierarchy



IT general controls—are applied to all IT service activities. For example, preventing unauthorized access to the computer system would protect all of the specific business processes that run on the computer (such as order entry/sales, billing/accounts receivable/cash receipts, inventory, payroll, and so on). We discuss pervasive control plans and general controls/IT general controls in Chapter 8.

PCAOB Auditing Standard No. 2, paragraphs 50–53, includes these first two levels within what the standard describes as "company-level-controls." These include controls such as the control environment and general controls (they use the term IT general controls). The standard emphasizes the pervasive affect that company-level controls

FIGURE 7.7 Lenox Control Matrix

	Control Goals of the Lenox Cash Receipts Business Process								
	Control Goals of the Operations Process				Control Goals of the Information Process				
Recommended control plans	Ensure effectiveness of operations		Ensure efficient employment of resources (e.g., people and computers)	Ensure security of resources (e.g., checks and AR data)	For the remittance advice inputs, ensure:			For the AR master data, ensure:	
	A	B			IV	IC	IA	UC	UA
P-1:	P-1					P-1			
P-n:			P-n					P-n	

Effectiveness goals include:

A – Timely deposit of checks

B – Comply with compensating balance agreements with the depository bank

IV = Input validity

IC = Input completeness

IA = Input accuracy

UC = Update completeness

UA = Update accuracy

have on the achievement of control objectives and the effectiveness of specific controls, such as business process controls. Many of these company-level controls, including IT general controls such as controls over computer program development, program change controls, controls over computer operations, and access to programs and data, are discussed in Chapter 8.

Business process control plans are applied to a particular business process, such as billing or cash receipts. **Application controls** are automated business process controls contained within IT application systems (i.e., computer programs). Business process control plans and application controls are introduced in Chapter 9 and discussed further in Chapters 10 through 14. We will use a control matrix, such as that in Figure 7.7, to match business process controls to the goals that we discussed previously. As you will learn in Chapter 9, a control matrix such as this will allow us to assess the effectiveness of design of the system of internal control by examining, easily, which goals are being addressed and which goals are not. See the cross-reference examples within the matrix (e.g., P-1 under A and IC, and P-n under efficient employment of resources and UC). Be careful, however, we use this matrix only to assess business process controls. You will learn more about this in Chapter 9.

Another useful and common way to classify controls is in relation to the timing of their occurrence. **Preventive control plans** stop problems from occurring. **Detective control plans** discover that problems have occurred. **Corrective control plans** rectify problems that have occurred. Let's use the Lenox process again to illustrate. The programmed verification of the customer number is an example of a *preventive* control; remittance advices with bad customer numbers should be rejected before they ever enter the computer system. A *detective* control is shown in the Lenox process at the manual processes (trapezoid symbol) labeled "Compare" in the Cashier column. The comparison is done to ensure that no discrepancies exist between inputs (endorsed checks) and the system outputs (deposit slips). If discrepancies are *detected*, Lenox should have a

procedure for reprocessing the incorrect items. This procedure would constitute a *corrective* control, which although not shown in Figure 7.4 (pg. 227) is alluded to with the annotation "Error routine not shown."

Obviously, if we had our choice, we would implement preventive controls because, in the long run, it is less expensive and less disruptive to operations to prevent, rather than to detect and correct, problems. However, because no control can be made to be 100 percent effective, we need to implement a combination of preventive, detective, and corrective controls. Furthermore, it should go without saying that detective control plans often can help to prevent or deter fraudulent or careless acts. That is, if someone knows that plans exist to detect or uncover fraud and carelessness, such knowledge can serve as one additional preventive measure.

Summary

In the introduction and in the section on fraud, we gave some alarming examples of fraud and computer crime incidences. Future managers must confront this problem much more directly than have their predecessors, particularly in light of recent business and audit failures, which gave rise to the Sarbanes-Oxley Act. Also, as computer-based systems become more sophisticated, managers must continually question how such technological changes affect the system of internal controls. For example, some companies have already implemented paperless (totally electronic) information systems. Others employ electronic data interchange (EDI) technology, which we introduced in Chapter 3. The challenges to future managers are to keep pace with the development of these types of systems and to ensure that changes in any process are complemented by enhancements in the company's system of internal controls.

Minimizing computer fraud and abuse is only one area of concern for today's managers. An organization's stakeholders—investors, customers, employees, taxpayers, government, and so on—have recently raised a number of *organizational governance* issues to demonstrate their interest in and concern over how well organizations are being managed. For example, these stakeholders are asking how well the board of directors (BOD) governs its own performance and that of the organization's managers. And, how do the BOD and management implement *and demonstrate* that they have control over their operations? We submit that only through an effective system of internal control can these and other matters be adequately addressed and suitably resolved.

Key Terms

organizational governance
Enterprise Risk Management (ERM)
risk
process
internal control
fraud
computer crime
computer virus
control environment
control matrix
control goals
effectiveness
efficiency
security of resources
input validity
input completeness
input accuracy
update completeness
update accuracy
control plans
pervasive control plans
general controls
IT general controls
business process control plans
application controls
preventive control plans
detective control plans
corrective control plans

Review Questions

RQ 7-1 Describe organizational governance.

RQ 7-2 Describe Enterprise Risk Management.

RQ 7-3 Describe the eight elements of Enterprise Risk Management.

RQ 7-4 Describe and compare risks and opportunities.

RQ 7-5 Describe four risk responses.

RQ 7-6 What gave rise to the Sarbanes-Oxley Act of 2002 (SOX)?

RQ 7-7 What are the key provisions of the Sarbanes-Oxley Act of 2002 (SOX)?

RQ 7-8 What is COSO?

RQ 7-9 Describe the elements common to most current definitions of internal control.

RQ 7-10 What is the relationship between fraud and internal control?

RQ 7-11 What is computer crime? Name and explain in your own words at least three ways that computer crimes have typically been committed.

RQ 7-12 What is a computer virus?

RQ 7-13 Explain what is meant by the *control environment*. What elements might comprise the control environment?

RQ 7-14 Explain how business ethics relate to internal control.

RQ 7-15 a. What are the three generic control goals of operations processes?

b. Explain the difference between the following pairs of control goals: (1) ensure effectiveness of operations processes and ensure efficient employment of resources; (2) ensure efficient employment of resources and ensure security of resources.

RQ 7-16 a. What are the five generic control goals of information processes?

b. Explain the difference between the following pairs of control goals: (1) ensure input validity and ensure input accuracy; (2) ensure input completeness and ensure input accuracy; (3) ensure input completeness and ensure update completeness; and (4) ensure input accuracy and ensure update accuracy.

RQ 7-17 What are the differences among the control environment, a pervasive control plan, and a business process control plan?

RQ 7-18 Distinguish among preventive, detective, and corrective control plans.

Discussion Questions

DQ 7-1 Recently, the U.S. federal government and the American Institute of Certified Public Accountants (AICPA) have taken aggressive steps aimed at ensuring the quality of organization governance. What are these changes, how might they change organization governance procedures, and do you believe that these actions will really improve internal control of business organizations?

DQ 7-2 ''Enterprise Risk Management is a process for organization governance.'' Discuss why this might be correct and why it might not.

DQ 7-3 Controls can be categorized as preventative, detective, and corrective. Assume that you are the controller for a large corporation. You are concerned about the controls related to the privacy of employee information, such as employees' social security numbers, salaries, benefits, medical histories, and so on. Name two preventive, two

detective, and two corrective controls you would design to ensure the privacy of sensitive employee information of this nature.

DQ 7-4 "If it weren't for the potential of computer crime, the emphasis on controlling computer systems would decline significantly in importance." Do you agree? Discuss fully.

DQ 7-5 Provide five examples of potential conflict between the control goals of ensuring effectiveness of operations and of ensuring efficient employment of resources.

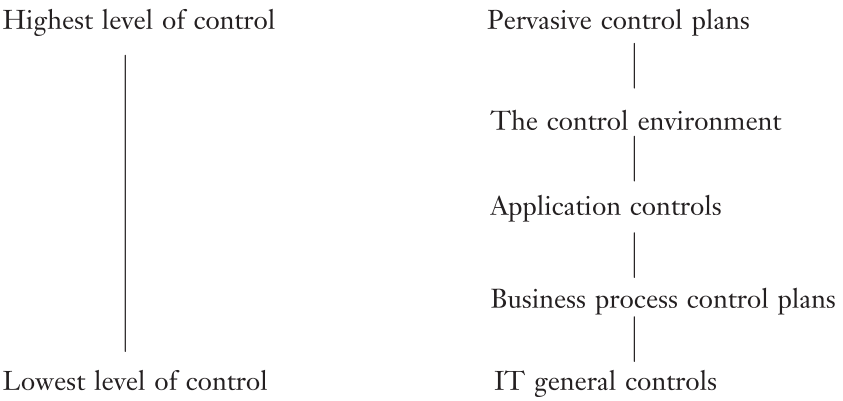
DQ 7-6 Discuss how the *efficiency* and *effectiveness* of a mass-transit system in a large city can be measured.

DQ 7-7 "If *input data* are entered into the system completely and accurately, then the information process control goals of *ensuring update completeness* and *ensuring update accuracy* will be automatically achieved." Do you agree? Discuss fully.

DQ 7-8 "Section 404 of the Sarbanes-Oxley Act of 2002 has not been a good idea. It has been too costly and it has not had its intended effect." Do you agree? Discuss fully.

DQ 7-9 How does this text's definition of internal control differ from COSO? How does it differ from the controls that are subject to review under Section 404 of the Sarbanes-Oxley Act of 2002?

DQ 7-10 What, if anything, is wrong with the following control hierarchy? Discuss fully.



Problems

P 7-1 Conduct research to determine management's responsibility for establishing and maintaining an adequate system of internal control. Create a written report, in a manner prescribed by your instructor, describing applicable statutory and professional guidance, the implications of internal control obligations, and how management should discharge its internal control responsibilities.

P 7-2 List 1 has 12 terms from this chapter, Chapter 1, or Chapter 3; List 2 contains 10 definitions or explanations of terms.

Match the definitions with the terms by placing a *capital* letter from list 1 on the blank line to the left of its corresponding definition in list 2. You should have three letters left over from list 1.

List 1—Terms

A. Business process control plan
B. Control environment

C. Control goal

D. Risk

E. Data maintenance update (of master data)

F. Information processing update (of master data)

G. Input accuracy

H. Input completeness

I. Input validity

J. Pervasive control plan

K. Preventive control plan

L. Operations process effectiveness goal

M. Application controls

List 2—Definitions

_____ 1. The process of modifying the master data reflects the results of new events.

_____ 2. A control designed to keep problems from occurring.

_____ 3. A control goal of the information process that is directed at ensuring that fictitious or bogus events are not recorded.

_____ 4. A goal of an operations process that signifies the very reason for which that process exists.

_____ 5. The highest level in the control *hierarchy*; a control category that evidences management's commitment to the importance of control in the organization.

_____ 6. The process of modifying a master data's *standing data*.

_____ 7. An automated control that is exercised within a business process as that process' events are processed.

_____ 8. An event that may cause an organization to fail to meet its objectives.

_____ 9. Objectives to be achieved by the internal control system.

____ 10. A control that addresses a multitude of goals across many business processes.

P 7-3 Following is a list of eight generic control goals from the chapter, followed by eight descriptions of either process failures (i.e., control goals not met) or instances of successful control plans (i.e., plans that helped to achieve control goals).

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

a. Place the *capital* letter of the control goal that *best* matches the situation described. One situation has two best answers.

2. Provide a one- or two-sentence explanation of how the situation relates to the control goal you selected.

   Hint: Some letters may be used more than once. Conversely, some letters may not apply at all.

Control Goals

A. Ensure effectiveness of operations

B. Ensure efficient employment of resources

C. Ensure security of resources

D. Ensure input validity

E. Ensure input completeness

F. Ensure input accuracy

G. Ensure update completeness

H. Ensure update accuracy

Situations

1. An accounts payable clerk at Woburn Company enters vendor invoices into the computer. When the invoices for a particular day were entered, the computer noted that vendor invoice 12345 appeared twice. The computer rejected the second entry (i.e., the duplicate, the invoice with the same number).

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

3. Instead of preparing deposit slips by hand, Lenox Company has them generated by the computer. The company does so to speed up the deposit of cash (speedy deposit being an objective at Lenox).

4. In the Lenox Company cash receipts process, one of the earliest processes is to endorse each customer's check with the legend, ''for deposit only to Lenox Company.''

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

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

7. At Otis Company, the accounts receivable master data is updated at the end of each day from payment data contained on the cash receipts event data store. At the completion of the update, run the difference between the total dollar value of AR before and after the update run is compared to the total dollars of payments being processed.

8. MiniScribe Corporation recorded as sales some shipments of disk drives between their warehouses. These disks drives had not been ordered by anyone and were still the property of MiniScribe.

P 7-4 In the following first list are 10 examples of the items described in the second list.

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

List 1—Examples

A. Management philosophy and operating style

B. Accounts receivable subsidiary ledger in a manual system

C. Customer name and address

D. The process of increasing customer balances for sales made

E. Cash receipts journal in a manual system

F. Fire extinguishers

G. Deleting an inactive customer's record from customer master data

H. Ensure input validity

I. Ensure security of resources

J. Computer virus

List 2—Descriptions

_____ 1. *Event data* in a computer system.

_____ 2. A control goal of the *information process.*

_____ 3. An element included in the *control environment.*

_____ 4. An element of *standing data.*

_____ 5. A control goal of an *operations process.*

_____ 6. An instance of *data maintenance.*

_____ 7. *Master data* in a computerized system.

_____ 8. An illustration of an *information processing update* (of master data).

P 7-5 The CFO of Synergein Corporation is very uncomfortable with its current risk exposure related to the possibility of business disruptions. Specifically, Synergein is heavily involved in e-business, and its internal information systems are tightly interlinked with its key customers' systems. The CFO has estimated that every hour of system downtime will cost the company about $10,000 in sales. The CFO and CIO (chief information officer) have further estimated that if the system were to fail, the average downtime would be 1 hour per incident. They have anticipated that Synergein will likely experience 50 downtime incidents in a given year due to internal computer system problems and another 50 incidents per year due to external

problems; specifically, system failures with the Internet service provider (ISP). Currently, Synergein pays an annualized cost of $150,000 for redundant computer and communication systems, and $100,000 for ISP support just to keep the total expected number of incidents to 100 per year.

Required:

a. Given the information provided thus far, how much ($) is the company's current *residual* expected *risk*?

b. A further preventative control would be to purchase and maintain more redundant computers and communication lines where possible, at an annualized cost of $100,000, which would reduce the expected number of downtime incidents to 15 per year due to internal computer system problems. What would be the dollar amount of Synergien's current *residual expected risk* at this point?

c. An external threat still prevails, that is, the ISP could cause the business interruption. Hence, another preventative control would be to increase the annual service fee the company pays to its ISP to a higher level of guaranteed service, based on the following schedule:

Guaranteed Maximum Number of Downtime Incidents per Year	Annual Cost of Service Support
50	$100,000 (current contract)
40	$150,000
30	$200,000
20	$300,000
10	$425,000
0	$550,000

Would you purchase a higher level of service from the ISP? If so, what level of service would you purchase? Please defend your answer both quantitatively and qualitatively.

P 7-6 Investigate the internal controls in one of the following (ask your instructor which): a local business, your home, your school, or your place of employment. Report (in a manner prescribed by your instructor) on the controls that you found and the goals that they were designed to achieve.

P 7-7 Figure 7.8 depicts the adaptation of a sample control matrix from a PricewaterhouseCoopers guide for Section 404 of the Sarbanes-Oxley Act of 2004.[21] We have added some data from the Lenox Company example to the

21 *Sarbanes-Oxley Act: Section 404 Practical Guidance for Management*. PricewaterhouseCoopers, July 2004, p. 105.

first row of the matrix. Compare the elements in Figure 7.8 to those in Figure 7.7 (pg. 234). What is similar? What is different?

FIGURE 7.8 PwC Sample Control Matrix for Problem 7-7

Sub-process	Control Objective	Description and Frequency of Control Activity	Financial Statement Area	Information Processing Objectives (C, A, V, R)[1]	Assertions (CO, EO, RO, VA, PD)[2]	P or D[3]	A or M[4]
Record cash receipts	Customer payments are accurate	The accounts receivable program verifies the accuracy of the payment data as it is entered by the accounts receivable clerk (daily)	Accounts receivable	A, V	EO, RO, VA	P	A

[1]Completeness (C), accuracy (A), validity (V), and restricted access (R).
[2]Completeness (C); existence or occurrence (EO); rights and obligations (RO); valuation and allocation (VA); and presentation and disclosure (PD).
[3]Preventive (P) or detective (D) control.
[4]Automated (A) or manual (M) control.