Chapter 3

Ethics, Fraud, and Internal Control

LEARNING OBJECTIVES

After studying this chapter, you should:

- Understand the broad issues pertaining to business ethics.
- Have a basic understanding of ethical issues related to the use of information technology.
- Be able to distinguish between management fraud and employee fraud.
- Be familiar with common types of fraud schemes.
- Be familiar with the key features of SAS 78/COSO internal control framework.
- Understand the objectives and application of physical controls.

This chapter examines three closely related areas of concern, which are specifically addressed by the Sarbanes-Oxley Act (SOX) and important to accountants and management. These are ethics, fraud, and internal control. We begin the chapter by surveying ethical issues that highlight the organization's conflicting responsibilities to its employees, shareholders, customers, and the general public. Organization managers have an ethical responsibility to seek a balance between the risks and benefits to these constituents that result from their decisions. Management and accountants must recognize the new implications of information technologies for such historic issues as working conditions, the right to privacy, and the potential for fraud. The section concludes with a review of the code of ethics requirements that SOX mandates.

The second section is devoted to the subject of fraud and its implications for accountants. Although the term *fraud* is very familiar in today's financial press, it is not always clear what constitutes fraud. In this section, we discuss the nature and meaning of fraud, differentiate between employee fraud and management fraud, explain fraud-motivating forces, review some common fraud techniques, and outline the key elements of the reform framework that SOX legislates to remedy these problems.

The final section in the chapter examines the subject of internal control. Both managers and accountants should be concerned about the adequacy of the organization's internal control structure as a means of deterring fraud and preventing errors. In this section, internal control issues are first presented on a conceptual level. We then discuss internal control within the context of the SAS 78/COSO framework recommended for SOX compliance.

Ethical Issues in Business

Ethical standards are derived from societal mores and deep-rooted personal beliefs about issues of right and wrong that are *not* universally agreed upon. It is quite possible for two individuals, both of whom consider themselves to be acting ethically, to be on opposite sides of an issue. Often, we confuse ethical issues with legal issues. When the Honorable Gentleman from the state of ——, who is charged with ethical misconduct, stands before Congress and proclaims that he is "guilty of no wrongdoing," is he really saying that he did not break the law?

We have been inundated with scandals in the stock market, stories of computer crimes and viruses, and almost obscene charges of impropriety and illegalities by corporate executives. Using covert compensation schemes, Enron's CFO Andy Fastow managed to improve his personal wealth by approximately $40 million. Similarly, Dennis Kozowski of Tyco, Richard Scrushy of HealthSouth, and Bernie Ebbers of WorldCom all became wealthy beyond imagination while driving their companies into the ground. Indeed, during the period from early 1999 to May 2002, the executives of 25 companies extracted $25 billion worth of special compensation, stock options, and private loans from their organizations while their companies' stock plummeted 75 percent or more.[1]

A thorough treatment of ethics issues is impossible within this chapter section. Instead, the objective of this section is to heighten the reader's awareness of ethical concerns relating to business, information systems, and computer technology.

Business Ethics

Ethics pertains to the principles of conduct that individuals use in making choices and guiding their behavior in situations that involve the concepts of right and wrong. More specifically, **business ethics** involves finding the answers to two questions: (1) How do managers decide what is right in conducting their business? and (2) Once managers have recognized what is right, how do they achieve it?

Ethical issues in business can be divided into four areas: equity, rights, honesty, and the exercise of corporate power. Table 3-1 identifies some of the business practices and decisions in each of these areas that have ethical implications.

Making Ethical Decisions

Business organizations have conflicting responsibilities to their employees, shareholders, customers, and the public. Every major decision has consequences that potentially harm or benefit these constituents. For example, implementing a new computer information system within an organization may cause some employees to lose their jobs, while those who remain enjoy the benefit of improved working conditions. Seeking a balance between these consequences is the managers' **ethical responsibility.** The following ethical principles provide some guidance in the discharge of this responsibility.[2]

Proportionality. The benefit from a decision must outweigh the risks. Furthermore, there must be no alternative decision that provides the same or greater benefit with less risk.

Justice. The benefits of the decision should be distributed fairly to those who share the risks. Those who do not benefit should not carry the burden of risk.

1 Robert Prentice, *Student Guide to the Sarbanes-Oxley Act*, Thomson Publishing, 2005, p. 23.
2 M. McFarland, "Ethics and the Safety of Computer System," *Computer* (February 1991).

TABLE 3-1 Ethical Issues in Business

Equity	Executive Salaries Comparable Worth Product Pricing
Rights	Corporate Due Process Employee Health Screening Employee Privacy Sexual Harassment Diversity Equal Employment Opportunity Whistleblowing
Honesty	Employee and Management Conflicts of Interest Security of Organization Data and Records Misleading Advertising Questionable Business Practices in Foreign Countries Accurate Reporting of Shareholder Interests
Exercise of Corporate Power	Political Action Committees Workplace Safety Product Safety Environmental Issues Divestment of Interests Corporate Political Contributions Downsizing and Plant Closures

Source: Adapted from: The Conference Board, "Defining Corporate Ethics," in P. Madsen and J. Shafritz, *Essentials of Business Ethics* (New York: Meridian, 1990), 18.

Minimize risk. Even if judged acceptable by the principles, the decision should be implemented so as to minimize all of the risks and avoid any unnecessary risks.

Computer Ethics

The use of information technology in business has had a major impact on society and thus raises significant ethical issues regarding computer crime, working conditions, privacy, and more. **Computer ethics** is "the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology. . . . [This includes] concerns about software as well as hardware and concerns about networks connecting computers as well as computers themselves."[3]

One researcher has defined three levels of computer ethics: pop, para, and theoretical.[4] Pop computer ethics is simply the exposure to stories and reports found in the

3 J. H. Moor, "What Is Computer Ethics?" *Metaphilosophy* 16 (1985): 266–75.

4 T. W. Bynum, "Human Values and the Computer Science Curriculum" (Working paper for the National Conference on Computing and Values, August 1991).

popular media regarding the good or bad ramifications of computer technology. Society at large needs to be aware of such things as computer viruses and computer systems designed to aid handicapped persons. Para computer ethics involves taking a real interest in computer ethics cases and acquiring some level of skill and knowledge in the field. All systems professionals need to reach this level of competency so they can do their jobs effectively. Students of accounting information systems should also achieve this level of ethical understanding. The third level, theoretical computer ethics, is of interest to multidisciplinary researchers who apply the theories of philosophy, sociology, and psychology to computer science with the goal of bringing some new understanding to the field.

A New Problem or Just a New Twist on an Old Problem?

Some argue that all pertinent ethical issues have already been examined in some other domain. For example, the issue of property rights has been explored and has resulted in copyright, trade secret, and patent laws. Although computer programs are a new type of asset, many feel that these programs should be considered no differently from other forms of property. A fundamental question arising from such debate is whether computers present new ethical problems or just create new twists on old problems. Where the latter is the case, we need only to understand the generic values that are at stake and the principles that should then apply.[5] However, a large contingent vociferously disagrees with the premise that computers are no different from other technology. For example, many reject the notion of intellectual property being the same as real property. There is, as yet, no consensus on this matter.

Several issues of concern for students of accounting information systems are discussed in the following section. This list is not exhaustive, and a full discussion of each of the issues is beyond the scope of this chapter. Instead, the issues are briefly defined, and several trigger questions are provided. Hopefully these questions will provoke thought and discussion in the classroom.

Privacy

People desire to be in full control of what and how much information about themselves is available to others, and to whom it is available. This is the issue of **privacy**. The creation and maintenance of huge, shared databases make it necessary to protect people from the potential misuse of data. This raises the issue of **ownership** in the personal information industry.[6] Should the privacy of individuals be protected through policies and systems? What information about oneself does the individual own? Should firms that are unrelated to individuals buy and sell information about these individuals without their permission?

Security (Accuracy and Confidentiality)

Computer **security** is an attempt to avoid such undesirable events as a loss of confidentiality or data integrity. Security systems attempt to prevent fraud and other misuse of computer systems; they act to protect and further the legitimate interests of the system's constituencies. The ethical issues involving security arise from the emergence of shared, computerized databases that have the potential to cause irreparable harm to individuals by disseminating inaccurate information to authorized users, such as through incorrect

5 G. Johnson, "A Framework for Thinking about Computer Ethics," in J. Robinette and R. Barquin (eds.), *Computers and Ethics: A Sourcebook for Discussions* (Brooklyn: Polytechnic Press, 1989): 26–31.

6 W. Ware, "Contemporary Privacy Issues" (Working paper for the National Conference on Computing and Human Values, August 1991).

credit reporting.[7] There is a similar danger in disseminating accurate information to persons unauthorized to receive it. However, increasing security can actually cause other problems. For example, security can be used both to protect personal property and to undermine freedom of access to data, which may have an injurious effect on some individuals. Which is the more important goal? Automated monitoring can be used to detect intruders or other misuse, yet it can also be used to spy on legitimate users, thus diminishing their privacy. Where is the line to be drawn? What is an appropriate use and level of security? Which is most important: security, accuracy, or confidentiality?

Ownership of Property

Laws designed to preserve real property rights have been extended to cover what is referred to as intellectual property, that is, software. The question here becomes what an individual (or organization) can own. Ideas? Media? Source code? Object code? A related question is whether owners and users should be constrained in their use or access. Copyright laws have been invoked in an attempt to protect those who develop software from having it copied. Unquestionably, the hundreds and thousands of program development hours should be protected from piracy. However, many believe the copyright laws can cause more harm than good. For example, should the look and feel of a software package be granted copyright protection? Some argue that this flies in the face of the original intent of the law. Whereas the purpose of copyrights is to promote the progress of science and the useful arts, allowing a user interface the protection of copyright may do just the opposite. The best interest of computer users is served when industry standards emerge; copyright laws work against this. Part of the problem lies in the uniqueness of software, its ease of dissemination, and the possibility of exact replication. Does software fit with the current categories and conventions regarding ownership?

Equity in Access

Some barriers to access are intrinsic to the technology of information systems, but some are avoidable through careful system design. Several factors, some of which are not unique to information systems, can limit access to computing technology. The economic status of the individual or the affluence of an organization will determine the ability to obtain information technology. Culture also limits access, for example, where documentation is prepared in only one language or is poorly translated. Safety features, or the lack thereof, have limited access to pregnant women, for example. How can hardware and software be designed with consideration for differences in physical and cognitive skills? What is the cost of providing equity in access? For what groups of society should equity in access become a priority?

Environmental Issues

Computers with high-speed printers allow for the production of printed documents faster than ever before. It is probably easier just to print a document than to consider whether it should be printed and how many copies really need to be made. It may be more efficient or more comforting to have a hard copy in addition to the electronic version. However, paper comes from trees, a precious natural resource, and ends up in landfills if not properly recycled. Should organizations limit nonessential hard copies? Can *nonessential* be defined? Who can and should define it? Should proper recycling be required? How can it be enforced?

---

7 K. C. Laudon, "Data Quality and Due Process in Large Interorganizational Record Systems," *Communications of the ACM* (1986): 4–11.

Artificial Intelligence

A new set of social and ethical issues has arisen out of the popularity of expert systems. Because of the way these systems have been marketed, that is, as decision makers or replacements for experts, some people rely on them significantly. Therefore, both knowledge engineers (those who write the programs) and domain experts (those who provide the knowledge about the task being automated) must be concerned about their responsibility for faulty decisions, incomplete or inaccurate knowledge bases, and the role given to computers in the decision-making process.[8] Further, because expert systems attempt to clone a manager's decision-making style, an individual's prejudices may implicitly or explicitly be included in the knowledge base. Some of the questions that need to be explored are: Who is responsible for the completeness and appropriateness of the knowledge base? Who is responsible for a decision made by an expert system that causes harm when implemented? Who owns the expertise once it is coded into a knowledge base?

Unemployment and Displacement

Many jobs have been and are being changed as a result of the availability of computer technology. People unable or unprepared to change are displaced. Should employers be responsible for retraining workers who are displaced as a result of the computerization of their functions?

Misuse of Computers

Computers can be misused in many ways. Copying proprietary software, using a company's computer for personal benefit, and snooping through other people's files are just a few obvious examples.[9] Although copying proprietary software (except to make a personal backup copy) is clearly illegal, it is commonly done. Why do people feel that it is not necessary to obey this law? Are there any good arguments for trying to change this law? What harm is done to the software developer when people make unauthorized copies? A computer is not an item that deteriorates with use, so is there any harm to the employer if it is used for an employee's personal benefit? Does it matter if the computer is used during company time or outside of work hours? Is there a difference if some profit-making activity takes place rather than, for example, using the computer to write a personal letter? Does it make a difference if a profit-making activity takes place during or outside of working hours? Is it okay to look through paper files that clearly belong to someone else? Is there any difference between paper files and computer files?

Sarbanes-Oxley Act and Ethical Issues

Public outcry surrounding ethical misconduct and fraudulent acts by executives of Enron, Global Crossing, Tyco, Adelphia, WorldCom, and others spurred Congress into passing the American Competitiveness and Corporate Accountability Act of 2002. This wide-sweeping legislation, more commonly known as the **Sarbanes-Oxley Act (SOX)**, is the most significant securities law since the SEC Acts of 1933 and 1934. SOX has many provisions designed to deal with specific problems relating to capital markets, corporate governance, and the

8 R. Dejoie, G. Fowler, and D. Paradice (eds.), *Ethical Issues in Information Systems* (Boston: Boyd & Fraser, 1991).

9 K. A. Forcht, "Assessing the Ethic Standards and Policies in Computer-Based Environments," in R. Dejoie, G. Fowler, and D. Paradice (eds.), *Ethical Issues in Information Systems* (Boston: Boyd & Fraser, 1991).

auditing profession. Several of these are discussed later in the chapter. At this point, we are concerned primarily with Section 406 of the act, which pertains to ethical issues.

Section 406—Code of Ethics for Senior Financial Officers

Section 406 of SOX requires public companies to disclose to the SEC whether they have adopted a code of ethics that applies to the organization's CEO, CFO, controller, or persons performing similar functions. If the company has not adopted such a code, it must explain why. A public company may disclose its code of ethics in several ways: (1) included as an exhibit to its annual report, (2) as a posting to its website, or (3) by agreeing to provide copies of the code upon request.

Whereas Section 406 applies specifically to executive and financial officers of a company, a company's code of ethics should apply equally to all employees. Top management's attitude toward ethics sets the tone for business practice, but it is also the responsibility of lower-level managers and nonmanagers to uphold a firm's ethical standards. Ethical violations can occur throughout an organization from the boardroom to the receiving dock. Methods must therefore be developed for including all management and employees in the firm's ethics schema. The SEC has ruled that compliance with Section 406 necessitates a written code of ethics that addresses the following ethical issues.

Conflicts of Interest. The company's code of ethics should outline procedures for dealing with actual or apparent conflicts of interest between personal and professional relationships. Note that the issue here is in dealing with conflicts of interest, not prohibiting them. Whereas avoidance is the best policy, sometimes conflicts are unavoidable. Thus, one's handling and full disclosure of the matter become the ethical concern. Managers and employees alike should be made aware of the firm's code of ethics, be given decision models, and participate in training programs that explore conflict of interest issues.

Full and Fair Disclosures. This provision states that the organization should provide full, fair, accurate, timely, and understandable disclosures in the documents, reports, and financial statements that it submits to the SEC and to the public. Overly complex and misleading accounting techniques were used to camouflage questionable activities that lie at the heart of many recent financial scandals. The objective of this rule is to ensure that future disclosures are candid, open, truthful, and void of such deceptions.

Legal Compliance. Codes of ethics should require employees to follow applicable governmental laws, rules, and regulations. As stated previously, we must not confuse ethical issues with legal issues. Nevertheless, doing the right thing requires sensitivity to laws, rules, regulations, and societal expectations. To accomplish this, organizations must provide employees with training and guidance.

Internal Reporting of Code Violations. The code of ethics must provide a mechanism to permit prompt internal reporting of ethics violations. This provision is similar in nature to Sections 301 and 806, which were designed to encourage and protect whistleblowers. Employee ethics hotlines are emerging as the mechanism for dealing with these related requirements. Because SOX requires this function to be confidential, many companies are outsourcing their employee hotline service to independent vendors.

Accountability. An effective ethics program must take appropriate action when code violations occur. This will include various disciplinary measures, including dismissal.

Employees must see an employee hotline as credible, or they will not use it. Section 301 directs the organization's audit committee to establish procedures for receiving, retaining, and treating such complaints about accounting procedures and internal control violations. Audit committees will also play an important role in the oversight of ethics enforcement activities.

Fraud and Accountants

Perhaps no major aspect of the independent auditor's role has caused more controversy than their responsibility for detecting fraud during an audit. In recent years, the structure of the U.S. financial reporting system has become the object of scrutiny. The SEC, the courts, and the public, along with Congress, have focused on business failures and questionable practices by the management of corporations that engage in alleged fraud. The question often asked is, "Where were the auditors?"

The passage of SOX has had a tremendous impact on the external auditor's responsibilities for fraud detection during a financial audit. It requires the auditor to test controls specifically intended to prevent or detect fraud likely to result in a material misstatement of the financial statements. The current authoritative guidelines on fraud detection are presented in **Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit*.** The objective of SAS 99 is to seamlessly blend the auditor's consideration of fraud into all phases of the audit process. In addition, SAS 99 requires the auditor to perform new steps such as a brainstorming during audit planning to assess the potential risk of material misstatement of the financial statements from fraud schemes.

Definitions of Fraud

Although *fraud* is a familiar term in today's financial press, its meaning is not always clear. For example, in cases of bankruptcies and business failures, alleged fraud is often the result of poor management decisions or adverse business conditions. Under such circumstances, it becomes necessary to clearly define and understand the nature and meaning of fraud.

Fraud denotes a false representation of a material fact made by one party to another party with the intent to deceive and induce the other party to justifiably rely on the fact to his or her detriment. According to common law, a fraudulent act must meet the following five conditions:

1. *False representation.* There must be a false statement or a nondisclosure.
2. *Material fact.* A fact must be a substantial factor in inducing someone to act.
3. *Intent.* There must be the intent to deceive or the knowledge that one's statement is false.
4. *Justifiable reliance.* The misrepresentation must have been a substantial factor on which the injured party relied.
5. *Injury or loss.* The deception must have caused injury or loss to the victim of the fraud.

Fraud in the business environment has a more specialized meaning. It is an intentional deception, misappropriation of a company's assets, or manipulation of its financial data to the advantage of the perpetrator. In accounting literature, fraud is also commonly known as *white-collar crime*, *defalcation*, *embezzlement*, and *irregularities*. Auditors encounter fraud at two levels: *employee fraud* and *management fraud*. Because each form of fraud has different implications for auditors, we need to distinguish between the two.

Employee fraud, or fraud by nonmanagement employees, is generally designed to directly convert cash or other assets to the employee's personal benefit. Typically, the employee circumvents the company's internal control system for personal gain. If a company has an effective system of internal control, defalcations or embezzlements can usually be prevented or detected.

Employee fraud usually involves three steps: (1) stealing something of value (an asset), (2) converting the asset to a usable form (cash), and (3) concealing the crime to avoid detection. The third step is often the most difficult. It may be relatively easy for a storeroom clerk to steal inventories from the employer's warehouse, but altering the inventory records to hide the theft is more of a challenge.

Management fraud is more insidious than employee fraud because it often escapes detection until the organization has suffered irreparable damage or loss. Usually management fraud does not involve the direct theft of assets. Top management may engage in fraudulent activities to drive up the market price of the company's stock. This may be done to meet investor expectations or to take advantage of stock options that have been loaded into the manager's compensation package. The Commission on Auditors' Responsibilities calls this performance fraud, which often involves deceptive practices to inflate earnings or to forestall the recognition of either insolvency or a decline in earnings. Lower-level management fraud typically involves materially misstating financial data and internal reports to gain additional compensation, to garner a promotion, or to escape the penalty for poor performance. Management fraud typically contains three special characteristics:[10]

1. The fraud is perpetrated at levels of management above the one to which internal control structures generally relate.
2. The fraud frequently involves using the financial statements to create an illusion that an entity is healthier and more prosperous than, in fact, it is.
3. If the fraud involves misappropriation of assets, it frequently is shrouded in a maze of complex business transactions, often involving related third parties.

The preceding characteristics of management fraud suggest that management can often perpetrate irregularities by overriding an otherwise effective internal control structure that would prevent similar irregularities by lower-level employees.

Factors that Contribute to Fraud

According to one study, people engage in fraudulent activity as a result of an interaction of forces both within an individual's personality and the external environment. These forces are classified into three major categories: (1) *situational pressures,* (2) *opportunities,* and (3) *personal characteristics (ethics)*. Figure 3-1 graphically displays the interplay of these three fraud-motivating forces.[11]

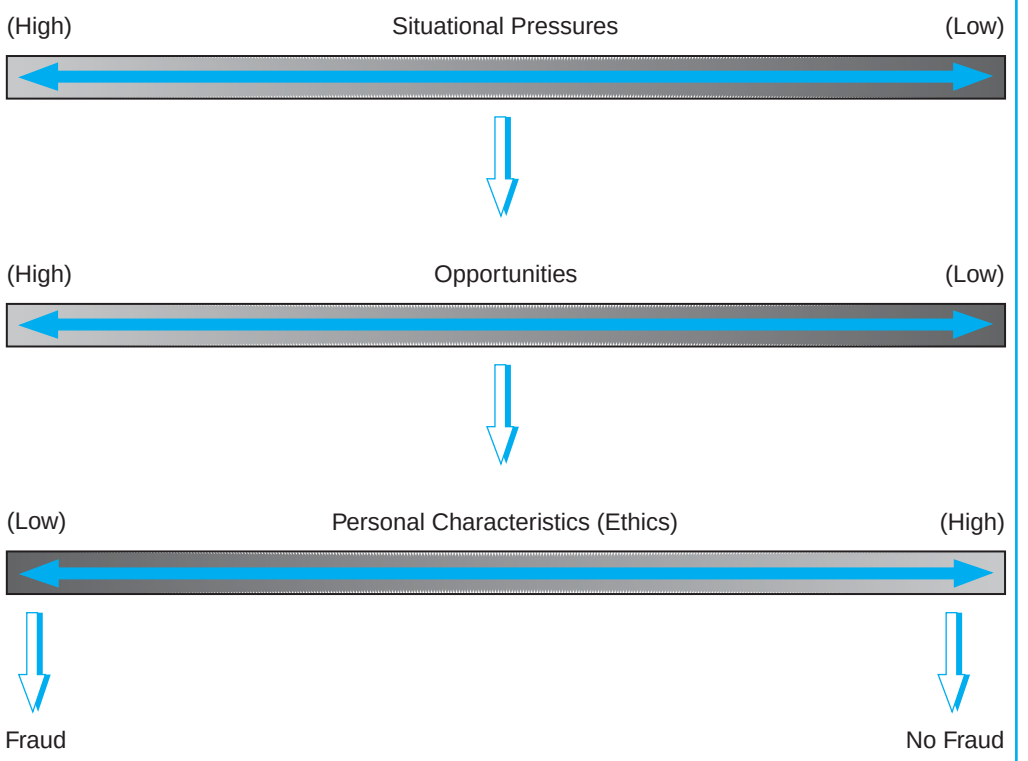
Figure 3-1 suggests that a person with a high level of personal ethics and limited pressure and opportunity to commit fraud is most likely to behave honestly. Similarly, an individual with lower ethical standards, when placed in situations with increasing pressure and given the opportunity, is most likely to commit fraud.

Whereas these factors, for the most part, fall outside of the auditors' sphere of influence, auditors can develop a *red-flag* checklist to detect possible fraudulent activity. To that end,

10 R. Grinaker, "Discussant's Response to a Look at the Record on Auditor Detection of Management Fraud," *Proceedings of the 1980 Touche Ross University of Kansas Symposium on Auditing Problems* (Kansas City: University of Kansas, 1980).

11 M. Romney, W. S. Albrecht, and D. J. Cherrington, "Auditors and the Detection of Fraud," *Journal of Accountancy* (May 1980).

FIGURE 3-1 Fraud-Motivating Forces



Source: Adapted from W. S. Albrecht and M. B. Romney, "Auditing Implications Derived from a Review of Cases and Articles Relating to Fraud," *Proceedings of the 1980 Touche Ross University of Kansas Symposium on Auditing Problems* (Kansas City: University of Kansas, 1980).

a questionnaire approach could be used to help external auditors uncover motivations for committing fraud. Some of the larger public accounting firms have developed checklists to help uncover fraudulent activity during an audit. Questions for such a checklist might include:[12]

- Do key executives have unusually high personal debt?
- Do key executives appear to be living beyond their means?
- Do key executives engage in habitual gambling?
- Do key executives appear to abuse alcohol or drugs?
- Do any of the key executives appear to lack personal codes of ethics?
- Are economic conditions unfavorable within the company's industry?
- Does the company use several different banks, none of which sees the company's entire financial picture?
- Do any key executives have close associations with suppliers?
- Is the company experiencing a rapid turnover of key employees, either through resignation or termination?
- Do one or two individuals dominate the company?

12 Ibid.

A review of some of these questions suggests that the contemporary auditor may use special investigative agencies to run a complete but confidential background check on the key managers of existing and prospective client firms.

Financial Losses from Fraud

A research study conducted by the Association of Certified Fraud Examiners (ACFE) in 2004 estimates losses from fraud and abuse to be 6 percent of annual revenues. This translates to approximately $660 billion. The actual cost of fraud is difficult to quantify for a number of reasons: (1) not all fraud is detected; (2) of that detected, not all is reported; (3) in many fraud cases, incomplete information is gathered; (4) information is not properly distributed to management or law enforcement authorities; and (5) too often, business organizations decide to take no civil or criminal action against the perpetrator(s) of fraud. In addition to the direct economic loss to the organization, indirect costs including reduced productivity, the cost of legal action, increased unemployment, and business disruption due to investigation of the fraud need to be considered.

Of the 508 cases examined in the ACFE study, more than half cost their victim organizations at least $100,000, and 15 percent caused losses of $1 million or more. The distribution of dollar losses is presented in Table 3-2.

The Perpetrators of Frauds

The ACFE study examined a number of factors that characterized the perpetrators of the frauds, including position within the organization, collusion with others, gender, age, and education. The median financial loss was calculated for each factor. The results of the study are summarized in Tables 3-3 through 3-7.

Fraud Losses by Position within the Organization

Table 3-3 shows that 68 percent of the reported fraud cases were committed by nonmanagerial employees, 34 percent by managers, and 12 percent by executives or owners. Although the number of reported fraud incidents perpetrated by employees is twice that of managers and five times that of executives, the average losses per category are inversely related.

TABLE 3-2 **Distribution of Losses**

Amount of Loss	Percent of Frauds
$1–$999	1.4
$1,000–$9,999	12.3
$10,000–$49,999	22.8
$50,000–$99,999	12.9
$100,000–$499,999	29.2
$500,000–$999,999	6.8
$1,000,000 and up	14.6

Source: Adapted from The Conference Board, "Defining Corporate Ethics," in P. Madsen and J. Shafritz, *Essentials of Business Ethics* (New York: Meridian, 1990), 18.

TABLE 3-3 Losses from Fraud by Position

Position	Percent of Frauds*	Loss
Owner/Executive	12	$900,000
Manager	34	140,000
Employee	68	62,000

*The sum of the percentages exceeds 100 because some of the reported frauds involved multiple perpetrators from more than one category.

TABLE 3-4 Losses from Fraud by Collusion

Perpetrators	Loss
Two or more (34.9%)	$200,000
One (65.1%)	58,500

TABLE 3-5 Losses from Fraud by Gender

Gender	Loss
Male	$160,000
Female	60,000

TABLE 3-6 Losses from Fraud by Age

Age Range	Loss
<25	$ 18,000
26–30	25,000
31–35	75,000
36–40	80,000
41–50	173,000
51–60	250,000
>60	527,000

TABLE 3-7 Losses from Fraud by Educational Level

Education Level	Loss
High school	$ 50,000
College	150,000
Post graduate	325,000

Fraud Losses and the Collusion Effect

Collusion among employees in the commission of a fraud is difficult to both prevent and detect. This is particularly true when the collusion is between managers and their subordinate employees. Management plays a key role in the internal control structure of an organization. They are relied upon to prevent and detect fraud among their subordinates. When they participate in fraud with the employees over whom they are supposed to provide oversight, the organization's control structure is weakened, or completely circumvented, and the company becomes more vulnerable to losses.

Table 3-4 compares the median losses from frauds that single individuals commit (regardless of position) and frauds involving collusion. This includes both internal collusion and schemes in which an employee or manager colludes with an outsider such as a vendor or a customer. Although fraud that a single perpertrator committed is far more common (65 percent of cases), the median loss from collusion is $200,000 as compared to $58,000 for frauds that an individual working alone perpetrated.

Fraud Losses by Gender

Table 3-5 shows that the median loss per case caused by males ($160,000) was almost three times that caused by females ($60,000).

Fraud Losses by Age

Table 3-6 indicates that perpetrators 25 years of age or younger caused median losses of about $18,000, while employees 60 and older perpetrated frauds that were on average 29 times larger—$527,000.

Fraud Losses by Education

Table 3-7 shows the median loss from frauds relative to the perpetrator's education level. Frauds committed by high school graduates averaged only $50,000, whereas those with bachelor's degrees averaged $150,000. Perpetrators with advanced degrees were responsible for frauds with a median loss of $325,000.

Conclusions to Be Drawn

Unless we intend to eliminate all managers and male employees over the age of 25 who have received degrees in higher education, the fraud classification scheme appears on the surface to provide little in the way of antifraud decision-making criteria. Upon closer examination, however, a common thread appears. Notwithstanding the importance of personal ethics and situational pressures, opportunity is the factor that most engenders fraud. Opportunity can be defined as control over assets or access to assets. Indeed, control and access are essential elements of opportunity. The financial loss differences associated with the previous classifications are explained by the opportunity factor.

- *Gender.* Whereas the demographic picture is changing, more men than women occupy positions of authority in business organizations, which provide them greater access to assets.
- *Position.* Those in the highest positions have the greatest access to company funds and assets.
- *Age.* Older employees tend to occupy higher-ranking positions and therefore generally have greater access to company assets.
- *Education.* Generally, those with more education occupy higher positions in their organizations and therefore have greater access to company funds and other assets.
- *Collusion.* One reason for segregating occupational duties is to deny potential perpetrators the opportunity they need to commit fraud. When individuals in critical positions collude, they create opportunities to control or gain access to assets that otherwise would not exist.

Fraud Schemes

Fraud schemes can be classified in a number of different ways. For purposes of discussion, this section presents the ACFE classification format. Three broad categories of fraud schemes are defined: fraudulent statements, corruption, and asset misappropriation.[13]

Fraudulent Statements

Fraudulent statements are associated with management fraud. Whereas all fraud involves some form of financial misstatement, to meet the definition under this class of fraud scheme the statement itself must bring direct or indirect financial benefit to the perpetrator. In other words, the statement is not simply a vehicle for obscuring or covering a fraudulent act. For example, misstating the cash account balance to cover the theft of cash is not financial statement fraud. On the other hand, understating liabilities to present a more favorable financial picture of the organization to drive up stock prices does fall under this classification.

Table 3-8 shows that whereas fraudulent statements account for only 8 percent of the fraud cases covered in the ACFE fraud study, the median loss due to this type of fraud scheme is significantly higher than losses from corruption and asset misappropriation.

Appalling as this type of fraud loss appears on paper, these numbers fail to reflect the human suffering that parallels them in the real world. How does one measure the impact on stockholders as they watch their life savings and retirement funds evaporate after news of the fraud breaks? The underlying problems that permit and aid these frauds are found in the boardroom, not the mail room. In this section, we examine some prominent corporate governance failures and the legislation to remedy them.

TABLE 3-8 Losses from Fraud by Scheme Type

Scheme Type	Percent of Frauds*	Loss
Fraudulent statements	8	$1,000,000
Corruption	30	250,000
Asset misappropriation	92	93,000

*The sum of the percentages exceeds 100 because some of the reported frauds in the ACFE study involved more than one type of fraud scheme.

13 *Report to the Nation: Occupational Fraud and Abuse.* (Association of Fraud Examiners, 2004): 31–34.

The Underlying Problems. The series of events symbolized by the Enron, WorldCom, and Adelphia debacles caused many to question whether our existing federal securities laws were adequate to ensure full and fair financial disclosures by public companies. The following underlying problems are at the root of this concern.

1. *Lack of Auditor Independence.* Auditing firms that are also engaged by their clients to perform nonaccounting activities such as actuarial services, internal audit outsourcing services, and consulting lack independence. The firms are essentially auditing their own work. The risk is that as auditors they will not bring to management's attention detected problems that may adversely affect their consulting fees. For example, Enron's auditors—Arthur Andersen—were also their internal auditors and their management consultants.
2. *Lack of Director Independence.* Many boards of directors are composed of individuals who are not independent. Examples of lack of independence are directors who have a personal relationship by serving on the boards of other directors' companies; have a business trading relationship as key customers or suppliers of the company; have a financial relationship as primary stockholders or have received personal loans from the company; or have an operational relationship as employees of the company.

   A notorious example of corporate inbreeding is Adelphia Communications, a telecommunications company. Founded in 1952, it went public in 1986 and grew rapidly through a series of acquisitions. It became the sixth largest cable provider in the United States before an accounting scandal came to light. The founding family (John Rigas, CEO and chairman of the board; Timothy Rigas, CFO, CAO, and chairman of the audit committee; Michael Rigas, VP for operation; and J.P. Rigas, VP for strategic planning) perpetrated the fraud. Between 1998 and May 2002, the Rigas family successfully disguised transactions, distorted the company's financial picture, and engaged in embezzlement that resulted in a loss of more than $60 billion to shareholders.

   Whereas it is neither practical nor wise to establish a board of directors that is totally void of self-interest, popular wisdom suggests that a healthier board of directors is one in which the majority of directors are independent outsiders with the integrity and the qualifications to understand the company and objectively plan its course.
3. *Questionable Executive Compensation Schemes.* A Thomson Financial survey revealed the strong belief that executives have abused stock-based compensation.[14] The consensus is that fewer stock options should be offered than currently is the practice. Excessive use of short-term stock options to compensate directors and executives may result in short-term thinking and strategies aimed at driving up stock prices at the expense of the firm's long-term health. In extreme cases, financial statement misrepresentation has been the vehicle to achieve the stock price needed to exercise the option.

   As a case in point, Enron's management was a firm believer in the use of stock options. Nearly every employee had some type of arrangement where they could purchase shares at a discount or were granted options based on future share prices. At Enron's headquarters in Houston, televisions were installed in the elevators so employees could track Enron's (and their own portfolio's) success. Before the firm's collapse, Enron executives added millions of dollars to their personal fortunes by exercising stock options.

14 Howard Stock, "Institutions Prize Good Governance: Once Bitten, Twice Shy, Investors Seek Oversight and Transparency," *Investor Relations Business* (New York: November 4, 2002).

4. *Inappropriate Accounting Practices.* The use of inappropriate accounting techniques is a characteristic common to many financial statement fraud schemes. Enron made elaborate use of special-purpose entities (SPEs) to hide liabilities through off-balance-sheet accounting. SPEs are legal, but their application in this case was clearly intended to deceive the market. Enron also employed income-inflating techniques. For example, when the company sold a contract to provide natural gas for a period of two years, they would recognize all the future revenue in the period when the contract was sold.

   WorldCom was another culprit of the improper accounting practices. In April 2001, WorldCom management decided to transfer transmission line costs from current expense accounts to capital accounts. This allowed them to defer some operating expenses and report higher earnings. Also, through acquisitions, they seized the opportunity to raise earnings. WorldCom reduced the book value of hard assets of MCI by $3.4 billion and increased goodwill by the same amount. Had the assets been left at book value, they would have been charged against earnings over four years. Goodwill, on the other hand, was amortized over a much longer period. In June 2002, the company declared a $3.8 billion overstatement of profits because of falsely recorded expenses over the previous five quarters. The size of this fraud increased to $9 billion over the following months as additional evidence of improper accounting came to light.

Sarbanes-Oxley Act and Fraud. To address plummeting institutional and individual investor confidence triggered in part by business failures and accounting restatements, Congress enacted SOX into law in July 2002. This landmark legislation was written to deal with problems related to capital markets, corporate governance, and the auditing profession and has fundamentally changed the way public companies do business and how the accounting profession performs its attest function. Some SOX rules became effective almost immediately, and others were phased in over time. In the short time since it was enacted, however, SOX is now largely implemented.

The act establishes a framework to modernize and reform the oversight and regulation of public company auditing. Its principal reforms pertain to (1) the creation of an accounting oversight board, (2) auditor independence, (3) corporate governance and responsibility, (4) disclosure requirements, and (5) penalties for fraud and other violations. These provisions are discussed in the following section.

1. *Accounting Oversight Board.* SOX created a **Public Company Accounting Oversight Board (PCAOB).** The PCAOB is empowered to set auditing, quality control, and ethics standards; to inspect registered accounting firms; to conduct investigations; and to take disciplinary actions.
2. *Auditor Independence.* The act addresses auditor independence by creating more separation between a firm's attestation and nonauditing activities. This is intended to specify categories of services that a public accounting firm cannot perform for its client. These include the following nine functions:
   (a) Bookkeeping or other services related to the accounting records or financial statements
   (b) Financial information systems design and implementation
   (c) Appraisal or valuation services, fairness opinions, or contribution-in-kind reports
   (d) Actuarial services
   (e) Internal audit outsourcing services
   (f) Management functions or human resources

(g) Broker or dealer, investment adviser, or investment banking services

(h) Legal services and expert services unrelated to the audit

(i) Any other service that the PCAOB determines is impermissible

Whereas SOX prohibits auditors from providing the above services to their audit clients, they are not prohibited from performing such services for nonaudit clients or privately held companies.

3. *Corporate Governance and Responsibility*. The act requires all audit committee members to be independent and requires the audit committee to hire and oversee the external auditors. This provision is consistent with many investors who consider the board composition to be a critical investment factor. For example, a Thomson Financial survey revealed that most institutional investors want corporate boards to be composed of at least 75 percent independent directors.[15]

   Two other significant provisions of the act relating to corporate governance are: (1) public companies are prohibited from making loans to executive officers and directors and (2) the act requires attorneys to report evidence of a material violation of securities laws or breaches of fiduciary duty to the CEO, CFO, or the PCAOB.

4. *Issuer and Management Disclosure*. SOX imposes new corporate disclosure requirements, including:

   (a) Public companies must report all off-balance-sheet transactions.

   (b) Annual reports filed with the SEC must include a statement by management asserting that it is responsible for creating and maintaining adequate internal controls and asserting to the effectiveness of those controls.

   (c) Officers must certify that the company's accounts "fairly present" the firm's financial condition and results of operations.

   (d) Knowingly filing a false certification is a criminal offense.

5. *Fraud and Criminal Penalties*. SOX imposes a range of new criminal penalties for fraud and other wrongful acts. In particular, the act creates new federal crimes relating to the destruction of documents or audit work papers, securities fraud, tampering with documents to be used in an official proceeding, and actions against whistleblowers.

Corruption

Corruption involves an executive, manager, or employee of the organization in collusion with an outsider. The ACFE study identifies four principal types of corruption: bribery, illegal gratuities, conflicts of interest, and economic extortion. Corruption accounts for about 10 percent of occupational fraud cases.

Bribery. **Bribery** involves giving, offering, soliciting, or receiving things of value to influence an official in the performance of his or her lawful duties. Officials may be employed by government (or regulatory) agencies or by private organizations. Bribery defrauds the entity (business organization or government agency) of the right to honest and loyal services from those employed by it. For example, the manager of a meat-packing company offers a U.S. health inspector a cash payment. In return, the inspector suppresses his report of health violations discovered during a routine inspection of the meat-packing facilities. In this situation, the victims are those who rely on the inspector's honest reporting.

15 Ibid.

The loss is salary paid to the inspector for work not performed and any damages that result from failure to perform.

Illegal Gratuities. An **illegal gratuity** involves giving, receiving, offering, or soliciting something of value because of an official act that has been taken. This is similar to a bribe, but the transaction occurs after the fact. For example, the plant manager in a large corporation uses his influence to ensure that a request for proposals is written in such a way that only one contractor will be able to submit a satisfactory bid. As a result, the favored contractor's proposal is accepted at a noncompetitive price. In return, the contractor secretly makes a financial payment to the plant manager. The victims in this case are those who expect a competitive procurement process. The loss is the excess costs the company incurs because of the noncompetitive pricing of the construction.

Conflicts of Interest. Every employer should expect that his or her employees will conduct their duties in a way that serves the interests of the employer. A **conflict of interest** occurs when an employee acts on behalf of a third party during the discharge of his or her duties or has self-interest in the activity being performed. When the employee's conflict of interest is unknown to the employer and results in financial loss, then fraud has occurred. The preceding examples of bribery and illegal gratuities also constitute conflicts of interest. This type of fraud can exist, however, when bribery and illegal payments are not present, but the employee has an interest in the outcome of the economic event. For example, a purchasing agent for a building contractor is also part owner in a plumbing supply company. The agent has sole discretion in selecting vendors for the plumbing supplies needed for buildings under contract. The agent directs a disproportionate number of purchase orders to his company, which charges above-market prices for its products. The agent's financial interest in the supplier is unknown to his employer.

Economic Extortion. **Economic extortion** is the use (or threat) of force (including economic sanctions) by an individual or organization to obtain something of value. The item of value could be a financial or economic asset, information, or cooperation to obtain a favorable decision on some matter under review. For example, a contract procurement agent for a state government threatens to blacklist a highway contractor if he does not make a financial payment to the agent. If the contractor fails to cooperate, the blacklisting will effectively eliminate him from consideration for future work. Faced with a threat of economic loss, the contractor makes the payment.

Asset Misappropriation

The most common form of fraud scheme involves some type of asset misappropriation. Ninety-two percent of the frauds included in the ACFE study fall in this category. Assets can be misappropriated either directly or indirectly for the perpetrator's benefit. Certain assets are more susceptible than others to misappropriation. Transactions involving cash, checking accounts, inventory, supplies, equipment, and information are the most vulnerable to abuse. Examples of fraud schemes involving asset misappropriation are described in the following sections.

Charges to Expense Accounts. The theft of an asset creates an imbalance in the basic accounting equation (assets = equities), which the criminal must adjust if the theft is to go undetected. The most common way to conceal the imbalance is to charge the asset to an expense account and reduce equity by the same amount. For example, the theft of $20,000 cash could be charged to a miscellaneous operating expense account. The loss of

the cash reduces the firm's assets by $20,000. To offset this, equity is reduced by $20,000 when the miscellaneous expense account is closed to retained earnings, thus keeping the accounting equation in balance. This technique has the advantage of limiting the criminal's exposure to one period. When the expense account is closed to retained earnings, its balance is reset to zero to begin the new period.

Lapping. **Lapping** involves the use of customer checks, received in payment of their accounts, to conceal cash previously stolen by an employee. For example, the employee first steals and cashes Customer A's check for $500. To conceal the accounting imbalance caused by the loss of the asset, Customer A's account is not credited. Later (the next billing period), the employee uses a $500 check received from Customer B and applies this to Customer A's account. Funds received in the next period from Customer C are then applied to the account of Customer B, and so on.

Employees involved in this sort of fraud often rationalize that they are simply borrowing the cash and plan to repay it at some future date. This kind of accounting cover-up must continue indefinitely or until the employee returns the funds. Lapping is usually detected when the employee leaves the organization or becomes sick and must take time off work. Unless the fraud is perpetuated, the last customer to have funds diverted from his or her account will be billed again, and the lapping technique will be detected. Employers can deter lapping by periodically rotating employees into different jobs and forcing them to take scheduled vacations.

Transaction Fraud. **Transaction fraud** involves deleting, altering, or adding false transactions to divert assets to the perpetrator. This technique may be used to ship inventories to the perpetrator in response to a fraudulent sales transaction or to disburse cash in payment of a false liability.

A common type of transaction fraud involves the distribution of fraudulent paychecks to nonexistent employees. For example, a supervisor keeps an employee who has left the organization on the payroll. Each week, the supervisor continues to submit time cards to the payroll department just as if the employee were still working. The fraud works best in organizations where the supervisor is responsible for distributing paychecks to employees. The supervisor may then forge the former employee's signature on the check and cash it. Although the organization has lost cash, the fraud can go undetected because the credit to the cash account is offset by a debit to payroll expense.

Computer Fraud Schemes. Because computers lie at the heart of most organizations' accounting information systems today, the topic of **computer fraud** is of special importance to auditors. Whereas the objectives of the fraud are the same—misappropriation of assets—the techniques used to commit computer fraud vary greatly.

No one knows the true extent of business losses each year due to computer fraud, but estimates reaching $100 billion per year give some indication of the problem's magnitude. One reason for uncertainty in loss estimates is that computer fraud is not well defined. For example, we saw in the ethics section of this chapter that some people do not view copying commercial computer software to be unethical. On the other side of this issue, software vendors consider this a criminal act. Regardless of how narrowly or broadly computer fraud is defined, most agree that it is a rapidly growing phenomenon.

For our purposes, computer fraud includes:

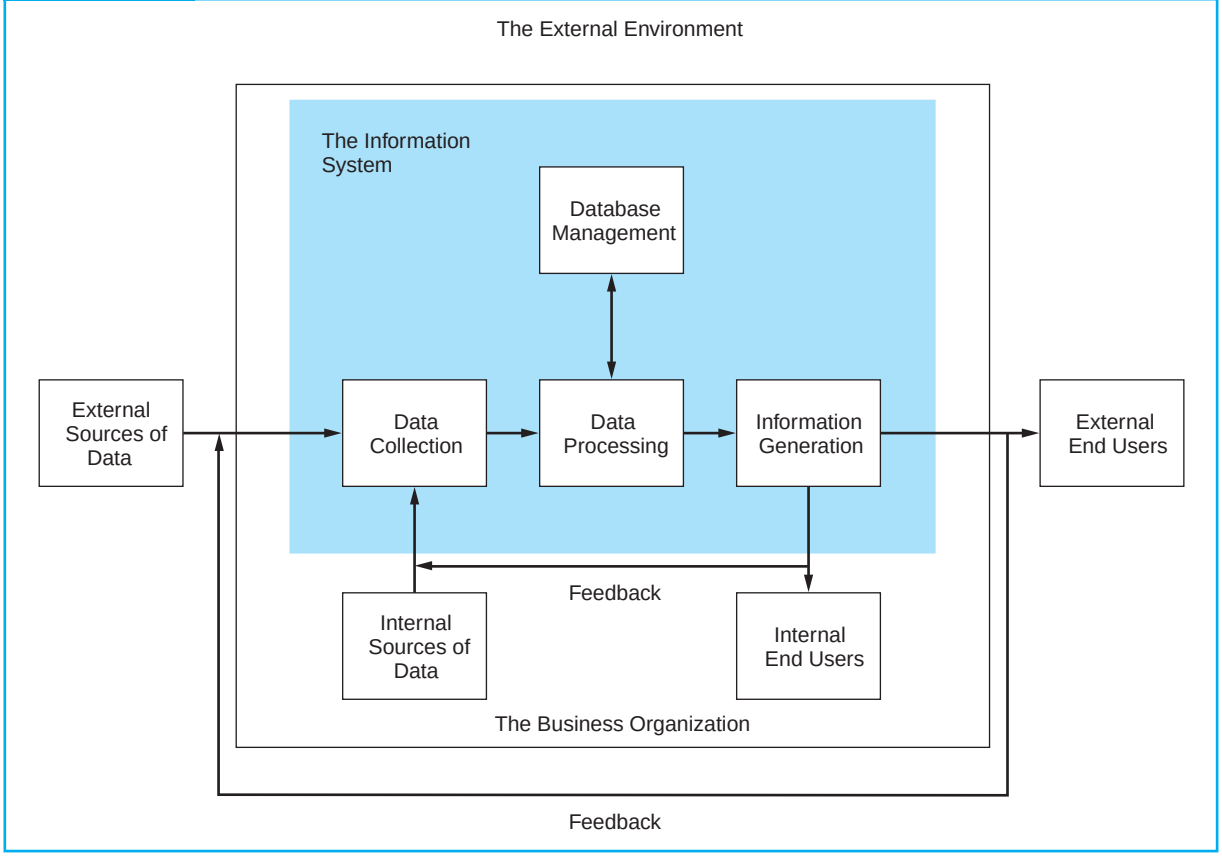
- The theft, misuse, or misappropriation of assets by altering computer-readable records and files.

- The theft, misuse, or misappropriation of assets by altering the logic of computer software.
- The theft or illegal use of computer-readable information.
- The theft, corruption, illegal copying, or intentional destruction of computer software.
- The theft, misuse, or misappropriation of computer hardware.

The general model for accounting information systems shown in Figure 3-2 conceptually portrays the key stages of an information system. Each stage in the model—data collection, data processing, database management, and information generation—is a potential area of risk for certain types of computer fraud.

Data Collection. **Data collection** is the first operational stage in the information system. The objective is to ensure that event data entering the system are valid, complete, and free from material errors. In many respects, this is the most important stage in the system. Should transaction errors pass through data collection undetected, the organization runs the risk that the system will process the errors and generate erroneous and unreliable output. This, in turn, could lead to incorrect actions and poor decisions by the users.

FIGURE 3-2 **The General Model for Accounting Information Systems**



Two rules govern the design of data collection procedures: relevance and efficiency. The information system should capture only relevant data. A fundamental task of the system designer is to determine what is and what is not relevant. He or she does so by analyzing the user's needs. Only data that ultimately contribute to information are relevant. The data collection stage should be designed to filter irrelevant facts from the system.

Efficient data collection procedures are designed to collect data only once. These data can then be made available to multiple users. Capturing the same data more than once leads to data redundancy and inconsistency. Information systems have limited collection, processing, and data storage capacity. Data redundancy overloads facilities and reduces the overall efficiency of the system. Inconsistency among data elements can result in inappropriate actions and bad decisions.

The simplest way to perpetrate a computer fraud is at the data collection or data entry stage. This is the computer equivalent of the transaction fraud discussed previously. Frauds of this type require little or no computer skills. The perpetrator need only understand how the system works to enter data that it will process. The fraudulent act involves falsifying data as it enters the system. This can be to delete, alter, or add a transaction. For example, to commit payroll fraud, the perpetrator may insert a fraudulent payroll transaction along with other legitimate transactions. Unless internal controls detect the insertion, the system will generate an additional paycheck for the perpetrator. A variation on this type of fraud is to change the Hours Worked field in an otherwise legitimate payroll transaction to increase the amount of the paycheck.

Still another variant on this fraud is to disburse cash in payment of a false account payable. By entering fraudulent supporting documents (purchase order, receiving report, and supplier invoice) into the data collection stage of the accounts payable system, a perpetrator can fool the system into creating an accounts payable record for a nonexistent purchase. Once the record is created, the system will presume it is legitimate and, on the due date, will disperse funds to the perpetrator in payment of a bogus liability.

Networked systems expose organizations to transaction frauds from remote locations. Masquerading, piggybacking, and hacking are examples of such fraud techniques. Masquerading involves a perpetrator gaining access to the system from a remote site by pretending to be an authorized user. This usually requires first gaining authorized access to a password. Piggybacking is a technique in which the perpetrator at a remote site taps in to the telecommunications lines and latches on to an authorized user who is logging in to the system. Once in the system, the perpetrator can masquerade as the authorized user. Hacking may involve piggybacking or masquerading techniques. Hackers are distinguished from other computer criminals because their motives are not usually to defraud for financial gain. They are motivated primarily by the challenge of breaking in to the system rather than the theft of assets. Nevertheless, hackers have caused extensive damage and loss to organizations. Many believe that the line between hackers and the more classic computer criminals is thin.

Data Processing. Once collected, data usually require processing to produce information. Tasks in the data processing stage range from simple to complex. Examples include mathematical algorithms (such as linear programming models) used for production scheduling applications, statistical techniques for sales forecasting, and posting and summarizing procedures used for accounting applications.

Data processing frauds fall into two classes: program fraud and operations fraud. **Program fraud** includes the following techniques: (1) creating illegal programs that can access data files to alter, delete, or insert values into accounting records; (2) destroying

or corrupting a program's logic using a computer virus; or (3) altering program logic to cause the application to process data incorrectly. For example, the program a bank uses to calculate interest on its customers' accounts will produce rounding errors. This happens because the precision of the interest calculation is greater than the reporting precision. Therefore, interest figures that are calculated to a fraction of one cent must be rounded to whole numbers for reporting purposes. A complex routine in the interest-calculation program keeps track of the rounding errors so that the total interest charge to the bank equals the sum of the individual credits. This involves temporarily holding the fractional amounts left over from each calculation in an internal memory accumulator. When the amount in the accumulator totals one cent (plus or minus), the penny is added to the customer's account that is being processed. In other words, one cent is added to (or deleted from) customer accounts randomly. A type of program fraud called the salami fraud involves modifying the rounding logic of the program so it no longer adds the one cent randomly. Instead, the modified program always adds the plus cent to the perpetrator's account but still adds the minus cent randomly. This can divert a considerable amount of cash to the perpetrator, but the accounting records stay in balance to conceal the crime.

Operations fraud is the misuse or theft of the firm's computer resources. This often involves using the computer to conduct personal business. For example, a programmer may use the firm's computer time to write software that he sells commercially. A CPA in the controller's office may use the company's computer to prepare tax returns and financial statements for her private clients. Similarly, a corporate lawyer with a private practice on the side may use the firm's computer to search for court cases and decisions in commercial databases. The cost of accessing the database is charged to the organization and hidden among other legitimate charges.

Database Management. The organization's database is its physical repository for financial and nonfinancial data. Database management involves three fundamental tasks: storage, retrieval, and deletion. The storage task assigns keys to new records and stores them in their proper location in the database. Retrieval is the task of locating and extracting an existing record from the database for processing. After processing is complete, the storage task restores the updated record to its place in the database. Deletion is the task of permanently removing obsolete or redundant records from the database.

Database management fraud includes altering, deleting, corrupting, destroying, or stealing an organization's data. Because access to database files is an essential element of this fraud, it is usually associated with transaction or program fraud. The most common technique is to access the database from a remote site and browse the files for useful information that can be copied and sold to competitors. Disgruntled employees have been known to destroy company data files simply to harm the organization. One method is to insert a destructive routine called a logic bomb into a program. At a specified time, or when certain conditions are met, the logic bomb erases the data files that the program accesses. For example, a disgruntled programmer who was contemplating leaving an organization inserted a logic bomb into the payroll system. Weeks later, when the system detected that the programmer's name had been removed from the payroll file, the logic bomb was activated and erased the payroll file.

Information Generation. Information generation is the process of compiling, arranging, formatting, and presenting information to users. Information can be an operational document such as a sales order, a structured report, or a message on a computer screen. Regardless of physical form, useful information has the following characteristics: **relevance, timeliness, accuracy, completeness,** and **summarization.**

- *Relevance.* The contents of a report or document must serve a purpose. This could be to support a manager's decision or a clerk's task. We have established that only data relevant to a user's action have information content. Therefore, the information system should present only relevant data in its reports. Reports containing irrelevancies waste resources and may be counterproductive to the user. Irrelevancies detract attention from the true message of the report and may result in incorrect decisions or actions.
- *Timeliness.* The age of information is a critical factor in determining its usefulness. Information must be no older than the time period of the action it supports. For example, if a manager makes decisions daily to purchase inventory from a supplier based on an inventory status report, then the information in the report should be no more than a day old.
- *Accuracy.* Information must be free from material errors. However, materiality is a difficult concept to quantify. It has no absolute value; it is a problem-specific concept. This means that in some cases, information must be perfectly accurate. In other instances, the level of accuracy may be lower. Material error exists when the amount of inaccuracy in information causes the user to make poor decisions or to fail to make necessary decisions. We sometimes must sacrifice absolute accuracy to obtain timely information. Often perfect information is not available within the decision time frame of the user. Therefore, in providing information, system designers seek a balance between information that is as accurate as possible, yet timely enough to be useful.
- *Completeness.* No piece of information essential to a decision or task should be missing. For example, a report should provide all necessary calculations and present its message clearly and unambiguously.
- *Summarization.* Information should be aggregated in accordance with a user's needs. Lower-level managers tend to need information that is highly detailed. As information flows upward through the organization to top management, it becomes more summarized. Later in this chapter, we will look more closely at the effects that organizational structure and managerial level have on information reporting.

A common form of fraud at the information generation stage is to steal, misdirect, or misuse computer output. One simple but effective technique called **scavenging** involves searching through the trash of the computer center for discarded output. A perpetrator can often obtain useful information from the carbon sheets removed from multipart reports or from paper reports that were rejected during processing. Sometimes output reports are misaligned on the paper or slightly garbled during printing. When this happens, the output must be reprinted, and the original output is often thrown in the trash.

Another form of fraud called **eavesdropping** involves listening to output transmissions over telecommunications lines. Technologies are readily available that enable perpetrators to intercept messages being sent over unprotected telephone lines and microwave channels. Most experts agree that it is practically impossible to prevent a determined perpetrator from accessing data communication channels. Data encryption can, however, render useless any data captured through eavesdropping.

Internal Control Concepts and Techniques

With the backdrop of ethics and fraud in place, let's now examine internal control concepts and techniques for dealing with these problems. The **internal control system**

comprises policies, practices, and procedures employed by the organization to achieve four broad objectives:

1. To safeguard assets of the firm.
2. To ensure the accuracy and reliability of accounting records and information.
3. To promote efficiency in the firm's operations.
4. To measure compliance with management's prescribed policies and procedures.[16]

Modifying Assumptions

Inherent in these control objectives are four modifying assumptions that guide designers and auditors of internal controls.[17]

Management Responsibility. This concept holds that the establishment and maintenance of a system of internal control is a **management responsibility**. This point is made eminent in SOX legislation.

Reasonable Assurance. The internal control system should provide **reasonable assurance** that the four broad objectives of internal control are met in a cost-effective manner. This means that no system of internal control is perfect and the cost of achieving improved control should not outweigh its benefits.

Methods of Data Processing. Internal controls should achieve the four broad objectives regardless of the data processing method used. The control techniques used to achieve these objectives will, however, vary with different types of technology.

Limitations. Every system of internal control has limitations on its effectiveness. These include (1) the possibility of error—no system is perfect, (2) circumvention—personnel may circumvent the system through collusion or other means, (3) management override—management is in a position to override control procedures by personally distorting transactions or by directing a subordinate to do so, and (4) changing conditions—conditions may change over time so that existing controls may become ineffectual.

Exposures and Risk

Figure 3-3 portrays the internal control system as a shield that protects the firm's assets from numerous undesirable events that bombard the organization. These include attempts at unauthorized access to the firm's assets (including information); fraud perpetrated by persons both inside and outside the firm; errors due to employee incompetence, faulty computer programs, and corrupted input data; and mischievous acts, such as unauthorized access by computer hackers and threats from computer viruses that destroy programs and databases.

The absence or weakness of a control is called an **exposure**. Exposures, which are illustrated as holes in the control shield in Figure 3-3, increase the firm's risk to financial loss or injury from undesirable events. A weakness in internal control may expose the

16 American Institute of Certified Public Accountants, *AICPA Professional Standards,* vol. 1 (New York: AICPA, 1987), AU Sec. 320.30–35.

17 American Institute of Certified Public Accountants, Committee on Auditing Procedure, Internal Control—Elements of a Coordinated System and Its Importance to Management and the Independent Public Accountant, *Statement on Auditing Standards* No. 1, Sec. 320 (New York: AICPA, 1973).

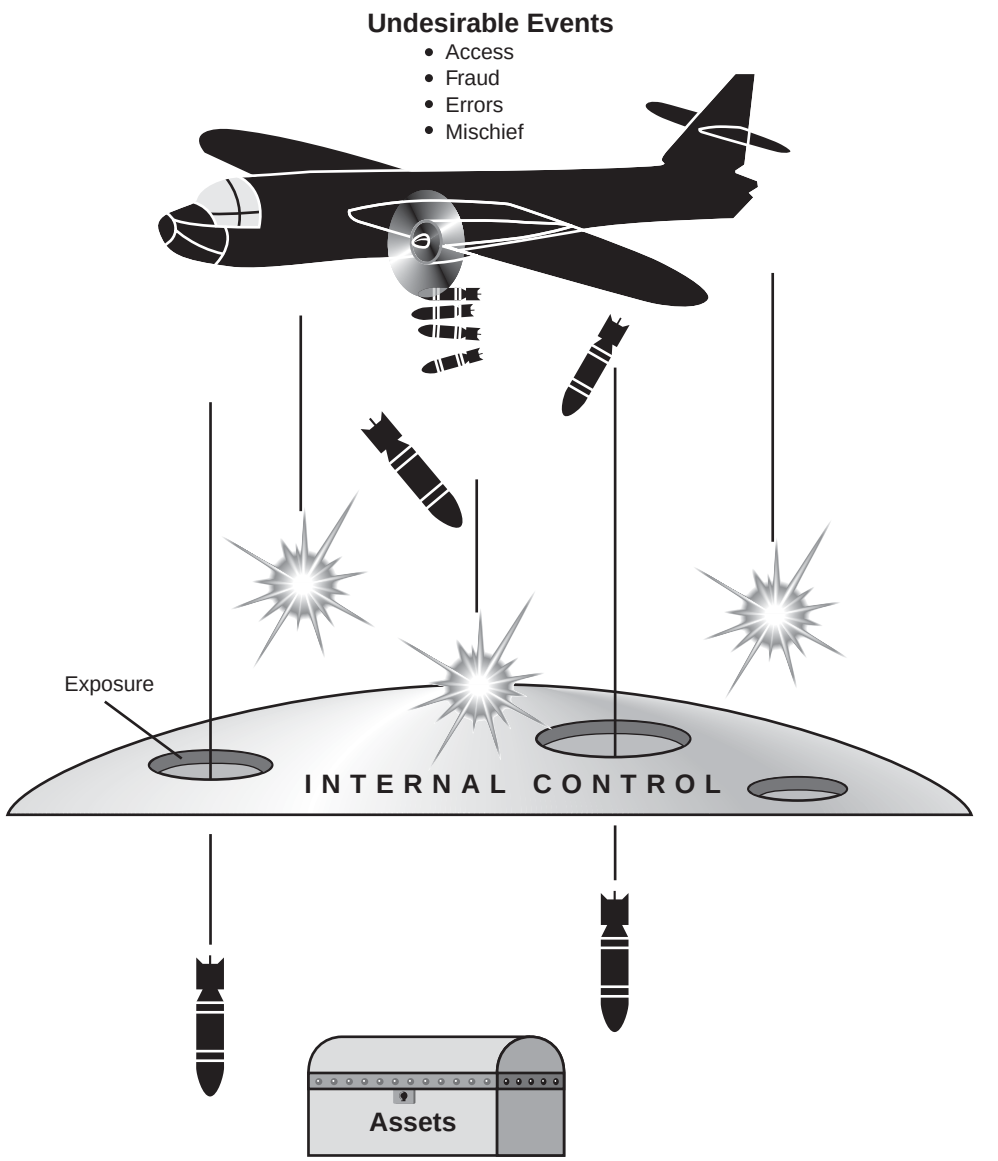
firm to one or more of the following types of risks:

1. Destruction of assets (both physical assets and information).
2. Theft of assets.
3. Corruption of information or the information system.
4. Disruption of the information system.

The Preventive–Detective–Corrective Internal Control Model

Figure 3-4 illustrates that the internal control shield is composed of three levels of control: preventive controls, detective controls, and corrective controls. This is the preventive–detective–corrective (PDC) control model.

FIGURE 3-3 **Internal Control Shield**

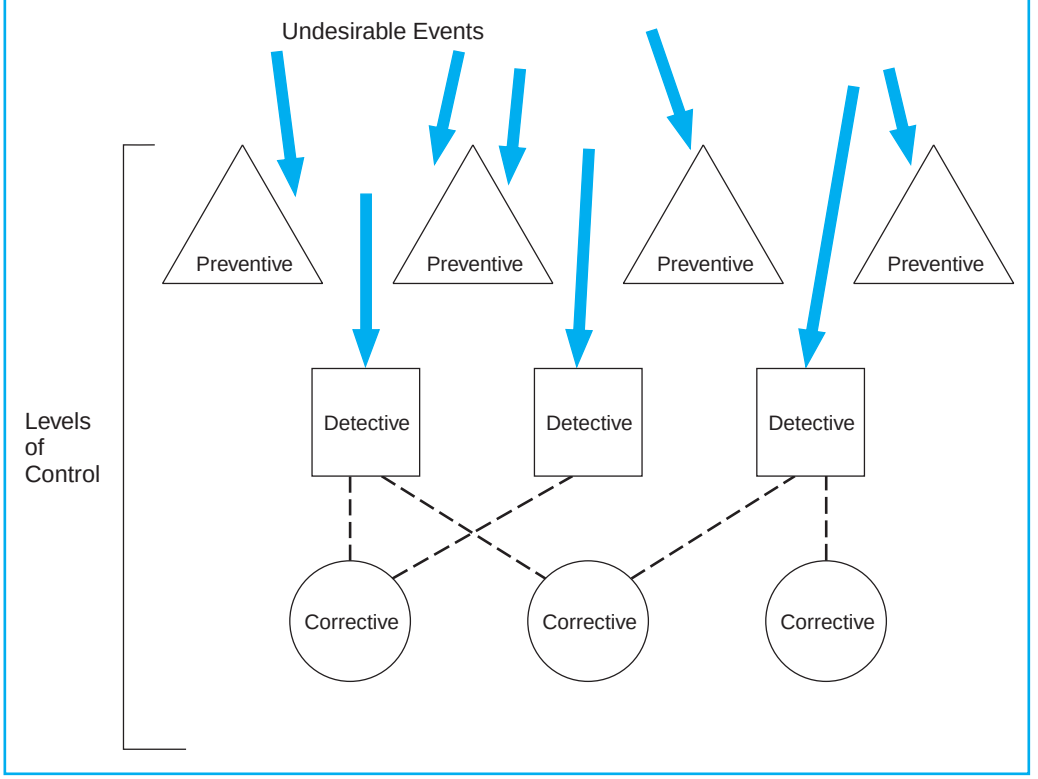


Preventive Controls. Prevention is the first line of defense in the control structure. **Preventive controls** are passive techniques designed to reduce the frequency of occurrence of undesirable events. Preventive controls force compliance with prescribed or desired actions and thus screen out aberrant events. When designing internal control systems, an ounce of prevention is most certainly worth a pound of cure. Preventing errors and fraud is far more cost-effective than detecting and correcting problems after they occur. The vast majority of undesirable events can be blocked at this first level. For example, a well-designed source document is an example of a preventive control. The logical layout of the document into zones that contain specific data, such as customer name, address, items sold, and quantity, forces the clerk to enter the necessary data. The source documents can therefore prevent necessary data from being omitted. However, not all problems can be anticipated and prevented. Some will elude the most comprehensive network of preventive controls.

Detective Controls. **Detective controls** form the second line of defense. These are devices, techniques, and procedures designed to identify and expose undesirable events that elude preventive controls. Detective controls reveal specific types of errors by comparing actual occurrences to pre-established standards. When the detective control identifies a departure from standard, it sounds an alarm to attract attention to the problem. For example, assume a clerk entered the following data on a customer sales order:

Quantity	Price	Total
10	$10	$1,000

FIGURE 3-4 **Preventive, Detective, and Corrective Controls**



Before processing this transaction and posting to the accounts, a detective control should recalculate the total value using the price and quantity. Thus the error in total price would be detected.

Corrective Controls. **Corrective controls** are actions taken to reverse the effects of errors detected in the previous step. There is an important distinction between detective controls and corrective controls. Detective controls identify anomalies and draw attention to them; corrective controls actually fix the problem. For any detected error, however, there may be more than one feasible corrective action, but the best course of action may not always be obvious. For example, in viewing the error above, your first inclination may have been to change the total value from $1,000 to $100 to correct the problem. This presumes that the quantity and price values on the document are correct; they may not be. At this point, we cannot determine the real cause of the problem; we know only that one exists.

Linking a corrective action to a detected error, as an automatic response, may result in an incorrect action that causes a worse problem than the original error. For this reason, error correction should be viewed as a separate control step that should be taken cautiously.

The PDC control model is conceptually pleasing but offers little practical guidance for designing specific controls. For this, we need a more precise framework. The current authoritative document for specifying internal control objectives and techniques is **Statement on Auditing Standards (SAS) No. 78**,[18] which is based on the COSO framework. We discuss the key elements of these documents in the following section.

Sarbanes-Oxley and Internal Control

Sarbanes-Oxley legislation requires management of public companies to implement an adequate system of internal controls over their financial reporting process. This includes controls over transaction processing systems that feed data to the financial reporting systems. Management's responsibilities for this are codified in Sections 302 and 404 of SOX. Section 302 requires that corporate management (including the CEO) certify their organization's internal controls on a quarterly and annual basis. In addition, Section 404 requires the management of public companies to assess the effectiveness of their organization's internal controls. This entails providing an annual report addressing the following points: (1) a statement of management's responsibility for establishing and maintaining adequate internal control; (2) an assessment of the effectiveness of the company's internal controls over financial reporting; (3) a statement that the organization's external auditors have issued an attestation report on management's assessment of the company's internal controls; (4) an explicit written conclusion as to the effectiveness of internal control over financial reporting;[19] and (5) a statement identifying the framework used in their assessment of internal controls.

Regarding the control framework to be used, both the PCAOB and the SEC have endorsed the framework put forward by the Committee of Sponsoring Organizations of

18 American Institute of Certified Public Accountants, SAS No. 78—*Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55* (New York: AICPA, 1995).

19 Management may not conclude that internal controls are effective if one or more material weaknesses exist. In addition, management must disclose all material weaknesses that exist as of the end of the most recent fiscal year.

the Treadway Commission (COSO). Further, they require that any other framework used should encompass all of COSO's general themes.[20] The COSO framework was the basis for SAS 78, but was designed as a management tool rather than an audit tool. SAS 78, on the other hand, was developed for auditors and describes the complex relationship between the firm's internal controls, the auditor's assessment of risk, and the planning of audit procedures. Apart from their audience orientation, the two frameworks are essentially the same and interchangeable for SOX compliance purposes. The key elements of the SAS 78/COSO framework are presented in the following section.

SAS 78/COSO Internal Control Framework

The SAS 78/COSO framework consists of five components: the control environment, risk assessment, information and communication, monitoring, and control activities.

The Control Environment

The **control environment** is the foundation for the other four control components. The control environment sets the tone for the organization and influences the control awareness of its management and employees. Important elements of the control environment are:

- The integrity and ethical values of management.
- The structure of the organization.
- The participation of the organization's board of directors and the audit committee, if one exists.
- Management's philosophy and operating style.
- The procedures for delegating responsibility and authority.
- Management's methods for assessing performance.
- External influences, such as examinations by regulatory agencies.
- The organization's policies and practices for managing its human resources.

SAS 78 requires that auditors obtain sufficient knowledge to assess the attitude and awareness of the organization's management, board of directors, and owners regarding internal control. The following paragraphs provide examples of techniques that may be used to obtain an understanding of the control environment.

1. Auditors should assess the integrity of the organization's management and may use investigative agencies to report on the backgrounds of key managers. Some of the "Big Four" public accounting firms employ ex-FBI agents whose primary responsibility is to perform background checks on existing and prospective clients. If cause for serious reservations comes to light about the integrity of the client, the auditor should withdraw from the audit. The reputation and integrity of the company's managers are critical factors in determining the auditability of the organization. Auditors cannot function properly in an environment in which client management is deemed unethical and corrupt.
2. Auditors should be aware of conditions that would predispose the management of an organization to commit fraud. Some of the obvious conditions may be lack of

20 A popular competing control framework is *Control Objectives for Information and related Technology* (COBIT®) published by the IT Governance Institute (ITGI). This framework maps into COSO's general themes.

sufficient working capital, adverse industry conditions, bad credit ratings, and the existence of extremely restrictive conditions in bank or indenture agreements. If auditors encounter any such conditions, their examination should give due consideration to the possibility of fraudulent financial reporting. Appropriate measures should be taken, and every attempt should be made to uncover any fraud.

3. Auditors should understand a client's business and industry and should be aware of conditions peculiar to the industry that may affect the audit. Auditors should read industry-related literature and familiarize themselves with the risks that are inherent in the business.
4. The board of directors should adopt, as a minimum, the provisions of SOX. In addition, the following guidelines represent established best practices.

   - *Separate CEO and chairman.* The roles of CEO and board chairman should be separate. Executive sessions give directors the opportunity to discuss issues without management present, and an independent chairman is important in facilitating such discussions.
   - *Set ethical standards.* The board of directors should establish a code of ethical standards from which management and staff will take direction. At a minimum, a code of ethics should address such issues as outside employment conflicts, acceptance of gifts that could be construed as bribery, falsification of financial and/or performance data, conflicts of interest, political contributions, confidentiality of company and customer data, honesty in dealing with internal and external auditors, and membership on external boards of directors.
   - *Establish an independent audit committee.* The audit committee is responsible for selecting and engaging an independent auditor, for ensuring that an annual audit is conducted, for reviewing the audit report, and for ensuring that deficiencies are addressed. Large organizations with complex accounting practices may need to create audit subcommittees that specialize in specific activities.
   - *Compensation committees.* The compensation committee should not be a rubber stamp for management. Excessive use of short-term stock options to compensate directors and executives may result in decisions that influence stock prices at the expense of the firm's long-term health. Compensation schemes should be carefully evaluated to ensure that they create the desired incentives.
   - *Nominating committees.* The board nominations committee should have a plan to maintain a fully staffed board of directors with capable people as it moves forward for the next several years. The committee must recognize the need for independent directors and have criteria for determining independence. For example, under its newly implemented governance standards, General Electric (GE) considers directors independent if the sales to, and purchases from, GE total less than 1 percent of the revenue of the companies where they serve as executives. Similar standards apply to charitable contributions from GE to any organization on which a GE director serves as officer or director. In addition, the company has set a goal that two-thirds of the board will be independent nonemployees.[21]

21 Rachel E. Silverman, "GE Makes Changes in Board Policy," *The Wall Street Journal* (New York: November 8, 2002).

- *Access to outside professionals.* All committees of the board should have access to attorneys and consultants other than the corporation's normal counsel and consultants. Under the provisions of SOX, the audit committee of an SEC reporting company is entitled to such representation independently.

Risk Assessment

Organizations must perform a **risk assessment** to identify, analyze, and manage risks relevant to financial reporting. Risks can arise or change from circumstances such as:

- Changes in the operating environment that impose new or changed competitive pressures on the firm.
- New personnel who have a different or inadequate understanding of internal control.
- New or reengineered information systems that affect transaction processing.
- Significant and rapid growth that strains existing internal controls.
- The implementation of new technology into the production process or information system that impacts transaction processing.
- The introduction of new product lines or activities with which the organization has little experience.
- Organizational restructuring resulting in the reduction and/or reallocation of personnel such that business operations and transaction processing are affected.
- Entering into foreign markets that may impact operations (that is, the risks associated with foreign currency transactions).
- Adoption of a new accounting principle that impacts the preparation of financial statements.

SAS 78 requires that auditors obtain sufficient knowledge of the organization's risk assessment procedures to understand how management identifies, prioritizes, and manages the risks related to financial reporting.

Information and Communication

The accounting information system (AIS) consists of the records and methods used to initiate, identify, analyze, classify, and record the organization's transactions and to account for the related assets and liabilities. The quality of information the AIS generates impacts management's ability to take actions and make decisions in connection with the organization's operations and to prepare reliable financial statements. An effective accounting information system will:

- Identify and record all valid financial transactions.
- Provide timely information about transactions in sufficient detail to permit proper classification and financial reporting.
- Accurately measure the financial value of transactions so their effects can be recorded in financial statements.
- Accurately record transactions in the time period in which they occurred.

SAS 78 requires that auditors obtain sufficient knowledge of the organization's information system to understand:

- The classes of transactions that are material to the financial statements and how those transactions are initiated.
- The accounting records and accounts that are used in the processing of material transactions.

- The transaction processing steps involved from the initiation of a transaction to its inclusion in the financial statements.
- The financial reporting process used to prepare financial statements, disclosures, and accounting estimates.

Monitoring

Management must determine that internal controls are functioning as intended. **Monitoring** is the process by which the quality of internal control design and operation can be assessed. This may be accomplished by separate procedures or by ongoing activities.

An organization's internal auditors may monitor the entity's activities in separate procedures. They gather evidence of control adequacy by testing controls and then communicate control strengths and weaknesses to management. As part of this process, internal auditors make specific recommendations for improvements to controls.

Ongoing monitoring may be achieved by integrating special computer modules into the information system that capture key data and/or permit tests of controls to be conducted as part of routine operations. Embedded modules thus allow management and auditors to maintain constant surveillance over the functioning of internal controls. In Chapter 17, we examine a number of embedded module techniques.

Another technique for achieving ongoing monitoring is the judicious use of management reports. Timely reports allow managers in functional areas such as sales, purchasing, production, and cash disbursements to oversee and control their operations. By summarizing activities, highlighting trends, and identifying exceptions from normal performance, well-designed management reports provide evidence of internal control function or malfunction. In Chapter 8, we review the management reporting system and examine the characteristics of effective management reports.

Control Activities

Control activities are the policies and procedures used to ensure that appropriate actions are taken to deal with the organization's identified risks. Control activities can be grouped into two distinct categories: IT controls and physical controls.

IT Controls. IT controls relate specifically to the computer environment. They fall into two broad groups: general controls and application controls. **General controls** pertain to entity-wide concerns such as controls over the data center, organization databases, systems development, and program maintenance. **Application controls** ensure the integrity of specific systems such as sales order processing, accounts payable, and payroll applications. Chapters 15, 16, and 17 are devoted to this extensive body of material. In the several chapters that follow, however, we shall see how physical control concepts apply in specific systems.

Physical Controls. This class of controls relates primarily to the human activities employed in accounting systems. These activities may be purely manual, such as the physical custody of assets, or they may involve the physical use of computers to record transactions or update accounts. Physical controls do not relate to the computer logic that actually performs accounting tasks. Rather, they relate to the human activities that trigger and utilize the results of those tasks. In other words, physical controls focus on people, but are not restricted to an environment in which clerks update paper accounts with pen and ink. Virtually all systems, regardless of their sophistication, employ human activities that need to be controlled.

Our discussion will address the issues pertaining to six categories of physical control activities: transaction authorization, segregation of duties, supervision, accounting records, access control, and independent verification.

Transaction Authorization. The purpose of **transaction authorization** is to ensure that all material transactions processed by the information system are valid and in accordance with management's objectives. Authorizations may be general or specific. General authority is granted to operations personnel to perform day-to-day operations. An example of general authorization is the procedure to authorize the purchase of inventories from a designated vendor only when inventory levels fall to their predetermined reorder points. This is called a programmed procedure (not necessarily in the computer sense of the word) where the decision rules are specified in advance, and no additional approvals are required. On the other hand, specific authorizations deal with case-by-case decisions associated with nonroutine transactions. An example of this is the decision to extend a particular customer's credit limit beyond the normal amount. Specific authority is usually a management responsibility.

Segregation of Duties. One of the most important control activities is the segregation of employee duties to minimize incompatible functions. **Segregation of duties** can take many forms, depending on the specific duties to be controlled. However, the following three objectives provide general guidelines applicable to most organizations. These objectives are illustrated in Figure 3-5.

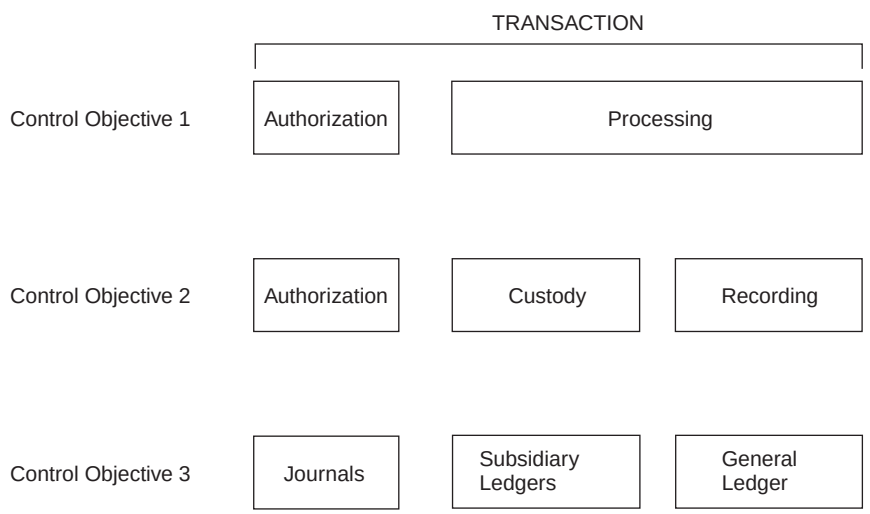
Objective 1. The segregation of duties should be such that the authorization for a transaction is separate from the processing of the transaction. For example, the purchasing department should not initiate purchases until the inventory control department gives authorization. This separation of tasks is a control to prevent individuals from purchasing unnecessary inventory.

Objective 2. Responsibility for the custody of assets should be separate from the record-keeping responsibility. For example, the department that has physical custody of finished goods inventory (the warehouse) should not keep the official inventory records. Accounting for finished goods inventory is performed by inventory control, an accounting function. When a single individual or department has responsibility for both asset custody and record keeping, the potential for fraud exists. Assets can be stolen or lost and the accounting records falsified to hide the event.

Objective 3. The organization should be structured so that a successful fraud requires collusion between two or more individuals with incompatible responsibilities. For example, no individual should have sufficient access to accounting records to perpetrate a fraud. Thus journals, subsidiary ledgers, and the general ledger are maintained separately. For most people, the thought of approaching another employee with the proposal to collude in a fraud presents an insurmountable psychological barrier. The fear of rejection and subsequent disciplinary action discourages solicitations of this sort. However, when employees with incompatible responsibilities work together daily in close quarters, the resulting familiarity tends to erode this barrier. For this reason, the segregation of incompatible tasks should be physical as well as organizational. Indeed, concern about personal familiarity on the job is the justification for establishing rules prohibiting nepotism.

Supervision. Implementing adequate segregation of duties requires that a firm employ a sufficiently large number of employees. Achieving adequate segregation of duties often presents difficulties for small organizations. Obviously, it is impossible to separate five

FIGURE 3-5 Segregation of Duties Objectives



incompatible tasks among three employees. Therefore, in small organizations or in functional areas that lack sufficient personnel, management must compensate for the absence of segregation controls with close **supervision**. For this reason, supervision is often called a compensating control.

An underlying assumption of supervision control is that the firm employs competent and trustworthy personnel. Obviously, no company could function for long on the alternative assumption that its employees are incompetent and dishonest. The competent and trustworthy employee assumption promotes supervisory efficiency. Firms can thus establish a managerial span of control whereby a single manager supervises several employees. In manual systems, maintaining a span of control tends to be straightforward because both manager and employees are at the same physical location.

Accounting Records. The **accounting records** of an organization consist of source documents, journals, and ledgers. These records capture the economic essence of transactions and provide an audit trail of economic events. The audit trail enables the auditor to trace any transaction through all phases of its processing from the initiation of the event to the financial statements. Organizations must maintain audit trails for two reasons. First, this information is needed for conducting day-to-day operations. The audit trail helps employees respond to customer inquiries by showing the current status of transactions in process. Second, the audit trail plays an essential role in the financial audit of the firm. It enables external (and internal) auditors to verify selected transactions by tracing them from the financial statements to the ledger accounts, to the journals, to the source documents, and back to their original source. For reasons of both practical expedience and legal obligation, business organizations must maintain sufficient accounting records to preserve their audit trails.

Access Control. The purpose of **access controls** is to ensure that only authorized personnel have access to the firm's assets. Unauthorized access exposes assets to misappropriation,

damage, and theft. Therefore, access controls play an important role in safeguarding assets. Access to assets can be direct or indirect. Physical security devices, such as locks, safes, fences, and electronic and infrared alarm systems, control against direct access. Indirect access to assets is achieved by gaining access to the records and documents that control the use, ownership, and disposition of the asset. For example, an individual with access to all the relevant accounting records can destroy the audit trail that describes a particular sales transaction. Thus, by removing the records of the transaction, including the account receivable balance, the sale may never be billed and the firm will never receive payment for the items sold. The access controls needed to protect accounting records will depend on the technological characteristics of the accounting system. Indirect access control is accomplished by controlling the use of documents and records and by segregating the duties of those who must access and process these records.

Independent Verification. **Verification procedures** are independent checks of the accounting system to identify errors and misrepresentations. Verification differs from supervision because it takes place after the fact, by an individual who is not directly involved with the transaction or task being verified. Supervision takes place while the activity is being performed, by a supervisor with direct responsibility for the task. Through independent verification procedures, management can assess (1) the performance of individuals, (2) the integrity of the transaction processing system, and (3) the correctness of data contained in accounting records. Examples of independent verifications include:

- Reconciling batch totals at points during transaction processing.
- Comparing physical assets with accounting records.
- Reconciling subsidiary accounts with control accounts.
- Reviewing management reports (both computer and manually generated) that summarize business activity.

The timing of verification depends on the technology employed in the accounting system and the task under review. Verifications may occur several times an hour or several times a day. In some cases, a verification may occur daily, weekly, monthly, or annually.

Summary

This chapter began by examining ethical issues that societies have pondered for centuries. It is increasingly apparent that good ethics is a necessary condition for the long-term profitability of a business. This requires that ethical issues be understood at all levels of the firm, from top management to line workers. In this section, we identified several ethical issues of direct concern to accountants and managers. SOX legislation has directly addressed these issues.

The next section examined fraud and its relationship to auditing. Fraud falls into two general categories: employee fraud and management fraud. Employee fraud is generally designed to convert cash or other assets directly to the employee's personal benefit. Typically, the employee circumvents the company's internal control structure for personal gain. However, if a company has an effective system of internal control, defalcations or embezzlements can usually be prevented or detected. Management fraud typically involves the material misstatement of financial data and reports to attain additional

compensation or promotion or to escape the penalty for poor performance. Managers that perpetrate fraud often do so by overriding the internal control structure. The underlying problems that permit and aid these frauds are frequently associated with inadequate corporate governance. In this section we examined some prominent corporate governance failures and outlined the key elements of SOX, which was legislated to remedy them. Finally, several well-documented fraud techniques were reviewed.

The third section examined the subject of internal control. The adequacy of the internal control structure is an issue of great importance to both management and accountants. Internal control was examined first using the PDC control model that classifies controls as preventive, detective, and corrective. Next, the SAS 78/COSO framework recommended for compliance with SOX was examined. This consists of five levels: control environment, risk assessment, information and communication, monitoring, and control activities. In this section, we focused on physical control activities including transaction authorization, segregation of duties, supervision, adequate accounting records, access control, and independent verification.

Key Terms

access controls (144)
accounting records (144)
accuracy (133)
application controls (142)
bribery (128)
business ethics (113)
completeness (133)
computer ethics (114)
computer fraud (130)
conflict of interest (129)
control activities (142)
control environment (139)
corrective controls (138)
data collection (131)
database management fraud (133)
detective controls (137)
eavesdropping (134)
economic extortion (129)
employee fraud (120)
ethical responsibility (113)
ethics (113)
exposure (135)
fraud (119)
general controls (142)
illegal gratuity (129)
internal control system (134)
lapping (130)
management fraud (120)
management responsibility (135)
monitoring (142)
operations fraud (132)
ownership (115)
preventive controls (137)
privacy (115)
program fraud (132)
Public Company Accounting Oversight Board (PCAOB) (127)
reasonable assurance (135)
relevance (133)
risk assessment (141)
Sarbanes-Oxley Act (SOX) (117)
scavenging (134)
security (115)
segregation of duties (143)
Statement on Auditing Standards (SAS) No. 78 (138)
Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (119)
summarization (133)
supervision (144)
timeliness (133)
transaction authorization (143)
transaction fraud (130)
verification procedures (145)

Review Questions

1. What is ethics?
2. What is business ethics?
3. What are the four areas of ethical business issues?
4. What are the main issues to be addressed in a business code of ethics required by the SEC?
5. What are three ethical principles that may provide some guidance for ethical responsibility?
6. What is computer ethics?
7. How do the three levels of computer ethics—pop, para, and theoretical—differ?
8. Are computer ethical issues new problems or just a new twist on old problems?
9. What are the computer ethical issues regarding privacy?
10. What are the computer ethical issues regarding security?
11. What are the computer ethical issues regarding ownership of property?
12. What are the computer ethical issues regarding equity in access?
13. What are the computer ethical issues regarding the environment?
14. What are the computer ethical issues regarding artificial intelligence?
15. What are the computer ethical issues regarding unemployment and displacement?
16. What are the computer ethical issues regarding misuse of computers?
17. What is the objective of SAS 99?
18. What are the five conditions that constitute fraud under common law?
19. Name the three fraud-motivating forces.
20. What is employee fraud?
21. What is management fraud?
22. What three forces within an individual's personality and the external environment interact to promote fraudulent activity?
23. How can external auditors attempt to uncover motivations for committing fraud?
24. What is lapping?
25. What is collusion?
26. What is bribery?
27. What is economic extortion?
28. What is conflict of interest?
29. What is computer fraud, and what types of activities does it include?
30. At which stage of the general accounting model is it easiest to commit computer fraud?
31. What are the four broad objectives of internal control?
32. What are the four modifying assumptions that guide designers and auditors of internal control systems?
33. Give an example of a preventive control.
34. Give an example of a detective control.
35. Give an example of a corrective control.
36. What are management's responsibilities under Sections 302 and 404?
37. What are the five internal control components described in the SAS 78/COSO framework?
38. What are the six broad classes of physical control activities defined by SAS 78?

Discussion Questions

1. Distinguish between ethical issues and legal issues.
2. Some argue against corporate involvement in socially responsible behavior because the costs incurred by such behavior place the organization at a disadvantage in a competitive market. Discuss the merits and flaws of this argument.
3. Although top management's attitude toward ethics sets the tone for business practice, sometimes it is the role of lower-level managers to uphold a firm's ethical standards. John, an operations-level manager, discovers that the company is illegally dumping toxic materials and is in violation of environmental regulations.

John's immediate supervisor is involved in the dumping. What action should John take?

4. When a company has a strong internal control structure, stockholders can expect the elimination of fraud. Comment on the soundness of this statement.
5. Distinguish between employee fraud and management fraud.
6. The estimates of losses annually due to computer fraud vary widely. Why do you think obtaining a good estimate of this figure is difficult?
7. How has the Sarbanes-Oxley Act had a significant impact on corporate governance?
8. Discuss the concept of exposure and explain why firms may tolerate some exposure.
9. If detective controls signal error flags, why shouldn't these types of controls automatically make a correction in the identified error? Why are corrective controls necessary?
10. Discuss the nonaccounting services that external auditors are no longer permitted to render to audit clients.
11. Discuss whether a firm with fewer employees than there are incompatible tasks should rely more heavily on general authority than specific authority.
12. An organization's internal audit department is usually considered an effective control mechanism for evaluating the organization's internal control structure. The Birch Company's internal auditing function reports directly to the controller. Comment on the effectiveness of this organizational structure.
13. According to SAS 78, the proper segregation of functions is an effective internal control procedure. Comment on the exposure (if any) caused by combining the tasks of paycheck preparation and distribution to employees.
14. Explain the five conditions necessary for an act to be considered fraudulent.
15. Distinguish between exposure and risk.
16. Explain the characteristics of management fraud.
17. The text identifies a number of personal traits of managers and other employees that might help uncover fraudulent activity. Discuss three.
18. Give two examples of employee fraud and explain how the thefts might occur.
19. Discuss the fraud schemes of bribery, illegal gratuities, and economic extortion.
20. Explain at least three forms of computer fraud.
21. Why are the computer ethics issues of privacy, security, and property ownership of interest to accountants?
22. A profile of fraud perpetrators prepared by the Association of Certified Fraud Examiners revealed that adult males with advanced degrees commit a disproportionate amount of fraud. Explain these findings.
23. Explain why collusion between employees and management in the commission of a fraud is difficult to both prevent and detect.
24. Because all fraud involves some form of financial misstatement, how is fraudulent statement fraud different?
25. Explain the problems associated with lack of auditor independence.
26. Explain the problems associated with lack of director independence.
27. Explain the problems associated with questionable executive compensation schemes.
28. Explain the problems associated with inappropriate accounting practices.
29. Explain the purpose of the PCAOB.
30. Why is an independent audit committee important to a company?
31. What are the key points of the "Issuer and Management Disclosure" of the Sarbanes-Oxley Act?
32. In this age of high technology and computer-based information systems, why are accountants concerned about physical (human) controls?

Multiple-Choice Questions

1. Management can expect various benefits to follow from implementing a system of strong internal control. Which of the following benefits is least likely to occur?
   a. reduction of cost of an external audit
   b. prevention of employee collusion to commit fraud
   c. availability of reliable data for decision-making purposes
   d. some assurance of compliance with the Foreign Corrupt Practices Act of 1977
   e. some assurance that important documents and records are protected
2. Which of the following situations is NOT a segregation of duties violation?
   a. The treasurer has the authority to sign checks but gives the signature block to the assistant treasurer to run the check-signing machine.
   b. The warehouse clerk, who has custodial responsibility over inventory in the warehouse, selects the vendor and authorizes purchases when inventories are low.
   c. The sales manager has the responsibility to approve credit and the authority to write off accounts.
   d. The department time clerk is given the undistributed payroll checks to mail to absent employees.
   e. The accounting clerk who shares the record-keeping responsibility for the accounts receivable subsidiary ledger performs the monthly reconciliation of the subsidiary ledger and the control account.
3. The underlying assumption of reasonable assurance regarding implementation of internal control means that
   a. by the control that fraud has not occurred in the period.
   b. auditors are reasonably assured that employee carelessness can weaken an internal control structure.
   c. implementation of the control procedure should not have a significant adverse effect on efficiency or profitability.
   d. management assertions about control effectiveness should provide auditors with reasonable assurance.
   e. a control applies reasonably well to all forms of computer technology.
4. To conceal the theft of cash receipts from customers in payment of their accounts, which of the following journal entries should the bookkeeper make?

	DR	CR
a.	Miscellaneous Expense	Cash
b.	Petty Cash	Cash
c.	Cash	Accounts Receivable
d.	Sales Returns	Accounts Receivable
e.	None of the above	

5. Which of the following controls would best prevent the lapping of accounts receivable?
   a. Segregate duties so that the clerk responsible for recording in the accounts receivable subsidiary ledger has no access to the general ledger.
   b. Request that customers review their monthly statements and report any unrecorded cash payments.
   c. Require customers to send payments directly to the company's bank.
   d. Request that customers make checks payable to the company.
6. Providing timely information about transactions in sufficient detail to permit proper classification and financial reporting is an example of
   a. the control environment.
   b. risk assessment.
   c. information and communication.
   d. monitoring.
7. Ensuring that all material transactions processed by the information system are valid and in accordance with management's objectives is an example of
   a. transaction authorization.
   b. supervision.

c. accounting records.
d. independent verification.

8. Which of the following is often called a compensating control?
   a. transaction authorization
   b. supervision
   c. accounting records
   d. independent verification
9. Which of the following is NOT a necessary condition under common law to constitute a fraudulent act?
   a. injury or loss
   b. material fact
   c. written documentation
   d. justifiable reliance
10. The fraud scheme that is similar to the "borrowing from Peter to pay Paul" scheme is
   a. expense account fraud.
   b. bribery.
   c. lapping.
   d. transaction fraud.

Problems

1. Fraud Scheme

A purchasing agent for a home improvement center is also part owner in a wholesale lumber company. The agent has sole discretion in selecting vendors for the lumber sold through the center. The agent directs a disproportionate number of purchase orders to his company, which charges above-market prices for its products. The agent's financial interest in the supplier is unknown to his employer.

Required:
What type of fraud is this and what controls can be implemented to prevent or detect the fraud?

2. Fraud Scheme

A procurement agent for a large metropolitan building authority threatens to blacklist a building contractor if he does not make a financial payment to the agent. If the contractor does not cooperate, the contractor will be denied future work. Faced with a threat of economic loss, the contractor makes the payment.

Required:
What type of fraud is this and what controls can be implemented to prevent or detect the fraud?

3. Mail Room Fraud and Internal Control

Sarat Sethi, a professional criminal, took a job as a mail room clerk at Benson & Abernathy and Company, a large department store. The mail room was an extremely hectic work environment consisting of a supervisor and 45 clerks. The clerks were responsible for handling promotional mailings, catalogs, and interoffice mail, as well as receiving and distributing a wide range of outside correspondence to various internal departments. One of Sethi's jobs was to open cash receipts envelopes from customers making payments on their credit card balances. He separated the remittance advices (the bills) and the checks into two piles. He then sent remittance advices to the accounts receivable department, where the customer accounts were updated to reflect the payment. He sent the checks to the cash receipts department, where they were recorded in the cash journal and then deposited in the bank. Batch totals of cash received and accounts receivable updated were reconciled each night to ensure that everything was accounted for. Nevertheless, over a one-month period Sethi managed to steal $100,000 in customer payments and then left the state without warning.

The fraud occurred as follows: Because the name of the company was rather long, some people had adopted the habit of making out checks simply to Benson. Sethi had a false ID prepared in the name of John Benson. Whenever he came across a check made out to Benson, he would steal it along

with the remittance advice. Sometimes people would even leave the payee section on the check blank. He also stole these checks. He would then modify the checks to make them payable to J. Benson and cash them. Because the accounts receivable department received no remittance advice, the end-of-day reconciliation with cash received disclosed no discrepancies.

Required:

a. This seems like a foolproof scheme. Why did Sethi limit himself to only one month's activity before leaving town?

b. What controls could Benson & Abernathy implement to prevent this from happening again?

4. Segregation of Duties

Explain why each of the following combinations of tasks should or should not be separated to achieve adequate internal control.

a. Approval of bad debt write-offs and the reconciliation of the accounts receivable subsidiary ledger and the general ledger control account.

b. Distribution of payroll checks to employees and approval of employee time cards.

c. Posting of amounts from both the cash receipts and the cash disbursements journals to the general ledger.

d. Writing checks to vendors and posting to the cash account.

e. Recording cash receipts in the journal and preparing the bank reconciliation.

5. Expense Account Fraud

While auditing the financial statements of Petty Corporation, the certified public accounting firm of Trueblue and Smith discovered that its client's legal expense account was abnormally high. Further investigation of the records indicated the following:

- Since the beginning of the year, several disbursements totaling $15,000 had been made to the law firm of Swindle, Fox, and Kreip.
- Swindle, Fox, and Kreip were not Petty Corporation's attorneys.
- A review of the canceled checks showed that they had been written and approved by Mary Boghas, the cash disbursements clerk.
- Boghas's other duties included performing the end-of-month bank reconciliation.
- Subsequent investigation revealed that Swindle, Fox, and Kreip are representing Mary Boghas in an unrelated embezzlement case in which she is the defendant. The checks had been written in payment of her personal legal fees.

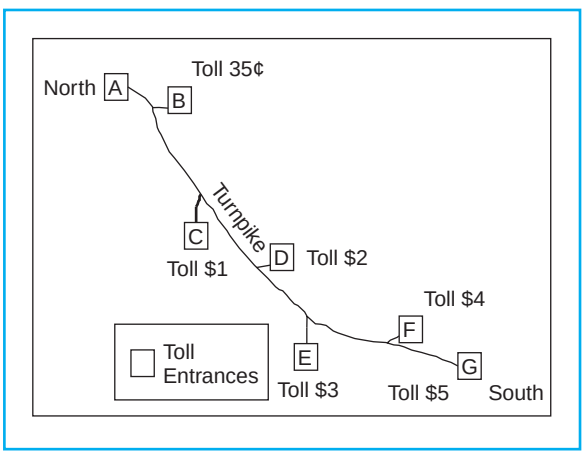
Required:

a. What control procedures could Petty Corporation have employed to prevent this unauthorized use of cash? Classify each control procedure in accordance with the SAS 78 framework (authorization, segregation of functions, supervision, and so on).

b. Comment on the ethical issues in this case.

6. Tollbooth Fraud

Collectors at Tollbooths A and B (see the following figure) have colluded to perpetrate a fraud. Each day, Tollbooth Collector B provides A with a number of toll tickets prestamped from Tollbooth B. The price of the toll from Point B to Point A is 35 cents. The fraud works as follows:



Drivers entering the turnpike at distant points south of Point B will pay tolls up to $5. When these drivers leave the turnpike at Point A, they pay the full amount of the toll printed on their tickets. However, the tollbooth collector replaces the tickets collected from the drivers with the 35-cent tickets provided by B, thus making it appear that the drivers entered the turnpike at Point B. The difference between the 35-cent tickets submitted as a record of the cash receipts and the actual amounts paid by the drivers is pocketed by Tollbooth Collector A and shared with B at the end of the day. Using this technique, Collectors A and B have stolen more than $20,000 in unrecorded tolls this year.

Required:
What control procedures could be implemented to prevent or detect this fraud? Classify the control procedures in accordance with SAS 78.

7. Factors of Fraud

Research has shown that situational pressures and opportunity are factors that contribute to fraudulent behavior.

Required:

a. Identify two situational pressures in a public company that would increase the likelihood of fraud.

b. Identify three opportunity situations that would increase the likelihood of fraud.

8. CMA 1289 3–4

Evaluation of Internal Control

Oakdale, Inc. is a subsidiary of Solomon Publishing and specializes in the publication and distribution of reference books. Oakdale's sales for the past year exceeded $18 million, and the company employed an average of 65 employees. Solomon periodically sends a member of the internal audit department to audit the operations of each of its subsidiaries, and Katherine Ford, Oakdale's treasurer, is currently working with Ralph Johnson of Solomon's internal audit staff. Johnson has just completed a review of Oakdale's investment cycle and prepared the following report.

General

Throughout the year, Oakdale has made both short-term and long-term investments in securities; all securities are registered in the company's name. According to Oakdale's bylaws, its board of directors must approve long-term investment activity, whereas either the president or the treasurer may approve short-term investment activity.

Transactions

The treasurer made all purchases and sales of short-term securities. The board approved the long-term security purchases, whereas the president approved the long-term security sale. Because the treasurer is listed with the broker as the company's contact, this individual received all revenue from these investments (dividends and interest) and then forwarded the checks to accounting for processing.

Documentation

The treasurer maintains purchase and sale authorizations, along with the broker's advices. The certificates for all long-term investments are kept in a safe deposit box at the local bank; only the president of Oakdale has access to this box. An inventory of this box was made, and all certificates were accounted for. Certificates for short-term investments are kept in a locked metal box in the accounting office. Other documents, such as long-term contracts and legal agreements, are also kept in this box. The president, the treasurer, and the accounting manager have the three keys to the box. The accounting manager's key is available to all accounting personnel should they require documents kept in this box. Documentation for two of the current short-term investments could not be located in this box; the accounting manager explained that some of the investments are for such short periods of time that the broker does not always provide formal documentation.

Accounting Records
The accounting department records deposits of checks for interest and dividends earned on investments, but these checks could not be traced to the cash receipts journal, which is maintained by the individual who normally opens, stamps, and logs incoming checks. These amounts are journalized monthly in an account for investment revenue. The treasurer authorizes checks drawn for investment purchases. Both the treasurer and the president must sign checks in excess of $15,000. When securities are sold, the broker deposits the proceeds directly in Oakdale's bank account by an electronic funds transfer.

Each month, the accounting manager and the treasurer prepare the journal entries required to adjust the short-term investment account. There was insufficient backup documentation attached to the journal entries reviewed to trace all transactions; however, the balance in the account at the end of last month closely approximates the amount shown on the statement received from the broker. The amount in the long-term investment account is correct, and the transactions can be clearly traced through the documentation attached to the journal entries. There are no attempts made to adjust either account to the lower of aggregate cost or market.

Required:
To achieve Solomon Publishing's objective of sound internal control, the company believes the following four controls are basic for an effective system of accounting control:

- Authorization of transactions
- Complete and accurate record keeping
- Access control
- Independent verification

a. Describe the purpose of each of the four controls listed above.
b. Identify an area in Oakdale's investment procedures that violates each of the four controls listed above.
c. For each of the violations identified, describe how Oakdale can correct each weakness.

9. Financial Aid Fraud

Harold Jones, the financial aid officer at a small university, manages all aspects of the financial aid program. Jones receives requests for aid from students, determines whether the students meet the aid criteria, authorizes aid payments, notifies the applicants that their request has been either approved or denied, writes the financial aid checks on the account he controls, and requires that the students come to his office to receive the checks in person. For years, Jones has used his position of authority to perpetrate the following fraud.

Jones encourages students who clearly will not qualify to apply for financial aid. Although the students do not expect aid, they apply on the off chance that it will be awarded. Jones modifies the financial information in the students' applications so that it falls within the established guidelines for aid. He then approves aid and writes aid checks payable to the students. The students, however, are informed that aid was denied. Because the students expect no aid, the checks in Jones's office are never collected. Jones forges the students' signatures and cashes the checks.

Required:
Identify the internal control procedures (classified per SAS 78) that could prevent or detect this fraud.

10. Kickback Fraud

The kickback is a form of fraud often associated with purchasing. Most organizations expect their purchasing agents to select the vendor that provides the best products at the lowest price. To influence the purchasing agent in his or her decision, vendors may grant the agent financial favors (cash, presents, football tickets, and so on). This activity can result in orders being placed with vendors that supply inferior products or charge excessive prices.

Required:
Describe the controls that an organization can employ to deal with kickbacks. Classify each control as preventive, detective, or corrective.

11. Evaluation of Controls

Gaurav Mirchandaniis is the warehouse manager for a large office supply wholesaler. Mirchandaniis receives two copies of the customer sales order from the sales department. He picks the goods from the shelves and sends them and one copy of the sales order to the shipping department. He then files the second copy in a temporary file. At the end of the day, Mirchandaniis retrieves the sales orders from the temporary file and updates the inventory subsidiary ledger from a terminal in his office. At that time, he identifies items that have fallen to low levels, selects a supplier, and prepares three copies of a purchase order. One copy is sent to the supplier, one is sent to the accounts payable clerk, and one is filed in the warehouse. When the goods arrive from the supplier, Mirchandaniis reviews the attached packing slip, counts and inspects the goods, places them on the shelves, and updates the inventory ledger to reflect the receipt. He then prepares a receiving report and sends it to the accounts payable department.

Required:

a. Prepare a systems flowchart of the procedures previously described.
b. Identify any control problems in the system.
c. What sorts of fraud are possible in this system?

12. Evaluation of Controls

Matt Demko is the loading dock supervisor for a dry cement packaging company. His work crew is composed of unskilled workers who load large transport trucks with bags of cement, gravel, and sand. The work is hard, and the employee turnover rate is high. Employees record their attendance on separate timecards. Demko authorizes payroll payments each week by signing the timecards and submitting them to the payroll department. Payroll then prepares the paychecks and gives them to Demko, who distributes them to his work crew.

Required:

a. Prepare a systems flowchart of the procedures described above.
b. Identify any control problems in the system.
c. What sorts of fraud are possible in this system?

Internal Control Cases

1. Bern Fly Rod Company

Bern Fly Rod Company is a small manufacturer of high-quality graphite fly-fishing rods. It sells its products to fly-fishing shops throughout the United States and Canada. Bern began as a small company with four salespeople, all family members of the owner. Due to the high popularity and recent growth of fly-fishing, Bern now employs a sales force of 16, and for the first time employs nonfamily members. The salespeople travel around the country giving fly-casting demos of their new models. Once the sales orders are generated, inventory availability is determined and, if necessary, the salesperson sends the order directly to the manufacturing department for immediate production. Sales staff compensation is tied directly to their sales figures. Bern's financial statements for the December year-end reflect unprecedented sales, 35 percent higher than last year. Further, sales for December account for 40 percent of all sales. Last year, December sales accounted for only 20 percent of all sales.

Required:

Analyze the previous situation and assess any potential internal control issues and exposures. Discuss some preventive measures this firm may wish to implement.

2. Breezy Company

(This case was prepared by Elizabeth Morris, Lehigh University)

Breezy Company of Bethlehem, Pennsylvania, is a small wholesale distributor of heating and cooling fans. The company deals with retailing firms that buy small to medium quantities of fans. The president, Chuck Breezy, was very pleased with the marked increase in sales over the past couple of years. Recently, however, the accountant informed Chuck that although net income has increased, the percentage of uncollectibles has tripled. Due to the small size of the business, Chuck fears he may not be able to sustain these increased losses in the future. He asked his accountant to analyze the situation.

Background

In 1998, the sales manager, John Breezy, moved to Alaska, and Chuck hired a young college graduate to fill the position. The company had always been a family business and, therefore, measurements of individual performance had never been a large consideration. The sales levels had been relatively constant because John had been content to sell to certain customers with whom he had been dealing for years. Chuck was leery about hiring outside of the family for this position. To try to keep sales levels up, he established a reward incentive based on net sales. The new sales manager, Bob Sellmore, was eager to set his career in motion and decided he would attempt to increase the sales levels. To do this, he recruited new customers while keeping the old clientele. After one year, Bob had proved himself to Chuck, who decided to introduce an advertising program to further increase sales. This brought in orders from a number of new customers, many of whom Breezy had never done business with before. The influx of orders excited Chuck so much that he instructed Jane Breezy, the finance manager, to raise the initial credit level for new customers. This induced some customers to purchase more.

Existing System

The accountant prepared a comparative income statement to show changes in revenues and expenses over the last three years, shown in Exhibit A. Currently, Bob is receiving a commission of 2 percent of net sales. Breezy Company uses credit terms of net 30 days. At the end of previous years, bad debt expense amounted to approximately 2 percent of net sales.

As the finance manager, Jane performs credit checks. In previous years, Jane had been familiar with most clients and approved credit on the basis of past behavior. When dealing with new customers, Jane usually approved a low credit amount and increased it after the customer exhibited reliability. With the large increase in sales, Chuck felt that the current policy was restricting a further rise in sales levels. He decided to increase credit limits to eliminate this restriction. This policy, combined with the new advertising program, should attract many new customers.

EXHIBIT A
BREEZY COMPANY
COMPARATIVE INCOME STATEMENT
FOR YEARS 2005, 2006, 2007

	2005	2006	2007
Revenues:			
Net sales	$350,000	$500,000	$600,000
Other revenue	60,000	60,000	62,000
Total revenue	410,000	560,000	662,000
Expenses:			
Cost of goods sold	140,000	200,000	240,000
Bad debt expense	7,000	20,000	36,000
Salaries expense	200,000	210,000	225,000
Selling expense	5,000	15,000	20,000
Advertising expense	0	0	10,000
Other expenses	20,000	30,000	35,000
Total expenses	372,000	475,000	566,000
Net income	$ 38,000	$ 85,000	$ 96,000

Future

The new level of sales impresses Chuck and he wishes to expand, but he also wants to keep uncollectibles to a minimum. He believes the amount of uncollectibles should remain relatively constant as a percentage of sales. Chuck is thinking of expanding his production line, but wants to see uncollectibles drop and sales stabilize before he proceeds with this plan.

Required:
Analyze the weaknesses in internal control and suggest improvements.

3. Whodunit?

(This case was prepared by Karen Collins, Lehigh University)

The following facts relate to an actual embezzlement case.

Someone stole more than $40,000 from a small company in less than two months. Your job is to study the following facts, try to figure out who was responsible for the theft, and how it was perpetrated, and (most important) suggest ways to prevent something like this from happening again.

Facts
Location of company: a small town on the eastern shore of Maryland. Type of company: crabmeat processor, selling crabmeat to restaurants located in Maryland. Characters in the story (names are fictitious):

- John Smith, president and stockholder (husband of Susan).
- Susan Smith, vice president and stockholder (wife of John).
- Tommy Smith, shipping manager (son of John and Susan).
- Debbie Jones, office worker. She began working part-time for the company six months before the theft. (At that time, she was a high school senior and was allowed to work afternoons through a school internship program.) Upon graduation from high school (several weeks before the theft was discovered), she began working full-time. Although she is not a member of the family, the Smiths have been close friends with Debbie's parents for more than 10 years.

Accounting Records
All accounting records are maintained on a microcomputer. The software being used consists of the following modules:

1. A general ledger system, which keeps track of all balances in the general ledger accounts and produces a trial balance at the end of each month.
2. A purchases program, which keeps track of purchases and maintains detailed records of accounts payable.
3. An accounts receivable program, which keeps track of sales and collections on account and maintains individual detailed balances of accounts receivable.
4. A payroll program.

The modules are not integrated (that is, data are not transferred automatically between modules). At the end of the accounting period, summary information generated by the purchases, accounts receivable, and payroll programs must be entered into the general ledger program to update the accounts affected by these programs.

Sales
The crabmeat processing industry in this particular town was unusual in that selling prices for crabmeat were set at the beginning of the year and remained unchanged for the entire year. The company's customers, all restaurants located within 100 miles of the plant, ordered the same quantity of crabmeat each week. Because prices for the crabmeat remained the same all year and the quantity ordered was always the same, the weekly invoice to each customer was always for the same dollar amount.

Manual sales invoices were produced when orders were taken, although these manual invoices were not prenumbered. One copy of the manual invoice was attached to the order shipped to the customer. The other copy was used to enter the sales information into the computer.

When the customer received the order, the customer would send a check to the company for the amount of the invoice. Monthly bills were not sent to customers unless the customer was behind in payments (that is, did not make a payment for the invoiced amount each week).

Note: The industry was unique in another way: many of the companies paid their

workers with cash each week (rather than by check). It was, therefore, not unusual for companies to request large sums of cash from the local banks.

When Trouble Was Spotted

Shortly after the May 30 trial balance was run, Susan began analyzing the balances in the various accounts. The balance in the cash account agreed with the cash balance she obtained from a reconciliation of the company's bank account.

However, the balance in the accounts receivable control account in the general ledger did not agree with the total of the accounts receivable subsidiary ledger (which shows a detail of the balances owed by each customer). The difference was not very large, but the balances should be in 100 percent agreement.

At this point, Susan hired a fraud auditor to help her locate the problem. In reviewing the computerized accounts receivable subsidiary ledger, the auditor noticed the following:

1. The summary totals from this report were not the totals that were entered into the general ledger program at month-end. Different amounts had been entered. No one could explain why this had happened.
2. Some sheets in the computer listing had been ripped apart at the bottom. (In other words, the listing of the individual accounts receivable balances was not a continuous list but had been split at several points.)
3. When an adding machine tape of the individual account balances was run, the individual balances did not add up to the total at the bottom of the report.

Susan concluded that the accounts receivable program was not running properly. The auditor's recommendation was that an effort be made to find out why the accounts receivable control account and the summary totals per the accounts receivable subsidiary ledger were not in agreement and why there were problems with the accounts receivable listing. Because the accounts receivable subsidiary and accounts receivable control account in the general ledger had been in agreement at the end of April, the effort should begin with the April ending balances for each customer by manually updating all of the accounts. The manually adjusted May 30 balances should then be compared with the computer-generated balances and any differences investigated.

After doing this, Susan and John found several differences. The largest difference was the following: Although they found the manual sales invoice for Sale 2, Susan and John concluded (based on the computer records) that Sale 2 did not take place. The auditor was not sure and recommended that they call this customer and ask him the following:

1. Did he receive this order?
2. Did he receive an invoice for it?
3. Did he pay for the order?
4. If so, did he have a copy of his canceled check?

Although John felt that this would be a waste of time, he called the customer. He received an affirmative answer to all of his questions. In addition, he found that the customer's check was stamped on the back with an address stamp giving only the company's name and city rather than the usual "for deposit only" company stamp. When questioned, Debbie said that she sometimes used this stamp.

Right after this question, Debbie, who was sitting nearby at the computer, called Susan to the computer and showed her the customer's account. She said that the payment for $5,000 was in fact recorded in the customer's account. The payments were listed on the computer screen like this:

Amount	Date of Payment
$5,000	May 3
$5,000	May 17
$5,000	May 23
$5,000	May 10

The auditor questioned the order of the payments—why was a check supposedly received on May 10 entered in the computer after checks received on May 17 and 23? About 30 seconds later, the computer malfunctioned and the accounts receivable file was lost.

Every effort to retrieve the file gave the message "file not found."

About five minutes later, Debbie presented Susan with a copy of a bank deposit ticket dated May 10 with several checks listed on it, including the check that the customer said had been sent to the company. The deposit ticket, however, was not stamped by the bank (which would have verified that the deposit had been received by the bank) and did not add up to the total at the bottom of the ticket (it was off by 20 cents).

At this point, being very suspicious, the auditor gathered all of the documents he could and left the company to work on the problem at home, away from any potential suspects. He received a call from Susan about four hours later saying that she felt much better. She and Debbie had gone to RadioShack (the maker of their computer program) and RadioShack had confirmed Susan's conclusion that the computer program was malfunctioning. She and Debbie were planning to work all weekend reentering transactions into the computer. She said that everything looked fine and not to waste more time and expense working on the problem.

The auditor felt differently. How do you feel?

Performance of Key Functions by Individual(s)

John, president
Susan, vice president
Tommy, son and shipping manager
Debbie, office worker

	Individual(s) Performing Task	
	Most of the Time	**Sometimes**
1. Receiving order from customers	John	All others
2. Overseeing production of crabmeat	John or Tommy	—
3. Handling shipping	Tommy	John
4. Billing customers (entering sales into accounts receivable program)	Debbie	Susan
5. Opening mail	John	All others
6. Preparing bank deposit tickets and making bank deposits	Susan or Debbie	All others
7. Recording receipt of cash and checks (entering collections of accounts receivable into accounts receivable program)	Debbie	Susan
8. Preparing checks (payroll checks and payments of accounts payable)	Susan or Debbie	—
9. Signing checks	John	—
10. Preparing bank reconciliations	John	—
11. Preparing daily sales reports showing sales by type of product	Susan	—
12. Summarizing daily sales reports to obtain monthly sales report by type of product	Susan or Debbie	—
13. Running summaries of AR program, AP program, and payroll program at month-end and inputting summaries into GL program	Susan or Debbie	—
14. Analyzing trial balance at month-end and analyzing open balances in accounts receivable and accounts payable	Susan	—

CUSTOMER ACCOUNT PER MANUAL RECONSTRUCTION

Dr.		Cr.	
Sale 1	5,000	Pmt. #1	5,000
Sale 2	5,000	Pmt. #2	5,000
Sale 3	5,000	Pmt. #3	5,000
Sale 4	5,000	–	–
Ending balance	5,000		

CUSTOMER ACCOUNT PER MANUAL RECONSTRUCTION

Dr.		Cr.	
Sale 1	5,000	Pmt. #1	5,000
Sale 2	5,000	Pmt. #2	5,000
Sale 3	5,000	Pmt. #3	5,000
Ending balance	0		

Required:

a. If you were asked to help this company, could you conclude from the evidence presented that embezzlement took place? What would you do next?

b. Who do you think was the embezzler?

c. How was the embezzlement accomplished?

d. What improvements would you recommend in internal control to prevent this from happening again? In answering this question, try to identify at least one suggestion from each of the six classes of internal control activities discussed in this chapter (in the Control Activities section): transaction authorization, segregation of duties, supervision, accounting records, access control, and independent verification.

e. Would the fact that the records were maintained on a microcomputer aid in this embezzlement scheme?