CHAPTER 3

Fighting Fraud: *An Overview*

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- **Become familiar with the different ways that organizations fight fraud.**
- **Understand the importance of fraud prevention.**
- **Understand how to create a culture of honesty and high ethics.**
- **Understand why hiring the right kind of employees can greatly reduce the risk of fraud.**
- **Understand how to assess and mitigate the risk of fraud.**
- **Understand the importance of early fraud detection.**
- **Understand different approaches to fraud investigation.**
- **Be familiar with the different options for legal action that can be taken once fraud has occurred.**

TO THE STUDENT

You should now understand the various types of fraud and fraud-fighting careers as well as those who commit fraud and why they do it. This chapter is a transition chapter to introduce you to the various ways in which organizations deal with fraud. The most cost-effective fraud-fighting activities involve preventing fraud from occurring. The second most cost-effective fraud-fighting activities involve implementing proactive approaches to detect fraud early, before it has a chance to grow. Once fraud has been detected (or there is *predication* that fraud might be occurring), organizations undertake various types of fraud investigation methods. After fraud has been investigated and the perpetrators are known, various types of legal action are possible. This chapter provides an overview of each of these activities. We then provide detailed coverage of these topics in the later chapters of this book. Fraud prevention is covered in Chapter 4; proactive fraud detection is the topic of Chapters 5 and 6; and fraud investigation is the focus of Chapters 7 through 10. Then, after discussing specific types of fraud in Chapters 11–17, we conclude the book with Chapter 18, which discusses legal actions that organizations can take against perpetrators. Essentially, this chapter provides an overview of the remainder of the book.

During the past two years, Mark-X Corporation has had three major frauds. The first involved a division manager overstating division profits by reporting fictitious revenues. Faced with declining sales and fearful of not meeting the level of sales to qualify for the company's bonus plan at the expense of being terminated, the manager inflated the amounts of service contracts to overstate revenues by $22 million. The second fraud was committed by the manager of the purchasing department. In his responsibility to secure uniforms for company employees, the manager gave favored treatment to a certain vendor. In return for allowing the vendor to charge higher prices and provide inferior goods, the vendor hired the purchasing manager's daughter as an "employee" and paid her over $400,000 for rendering no service. In fact, when investigated, the daughter didn't even know the location of the vendor's offices or telephone number (for whom she supposedly worked). As an "employee" the daughter funneled bribes to her father, the purchasing agent. As a result of this kickback scheme, Mark-X purchased $11 million of uniforms at inflated prices. The third fraud involved two warehouse managers stealing approximately $300,000 in inventory. This fraud was perpetrated by issuing credit memos to customers who supposedly returned defective merchandise and were given product replacements. In fact, the merchandise was never returned. The credit memos were used to conceal the theft of "high value" merchandise from the warehouse.

All three of these frauds were uncovered and brought significant embarrassment to the company's management and board of directors. The three frauds also cost the company a tremendous amount of money to investigate. In a board of directors meeting, the chairman of the board made the following comment to the CEO: "I am sick and tired of these fraud surprises hitting the newspapers. If there is one more high-profile fraud in this company, I will be resigning from the board and recommending that you be replaced as CEO."

Following the board meeting, the CEO called an emergency meeting with the CFO, the internal audit director, in-house legal counsel, and the director of corporate security. In the meeting, he told them that unless the company successfully developed a proactive fraud prevention and detection program, all of them would lose their jobs. He reviewed the three major frauds and told them what the chairman of the board had said. His final words were, "I don't care how much you spend, I want the best proactive, fraud-mitigating program possible. Hire whatever consultants you need, but get me a proactive fraud program that I can report to the board, and do it quickly."

Knowing Different Ways That Organizations Fight Fraud

Assume that you are the fraud-fighting consultant hired by the company. What advice would you give this company? What kind of fraud prevention, detection, and investigation programs would you recommend be implemented? What kind of ethics programs would you put in place? What kind of prosecution policies would you establish? A consultant would probably start by telling the management of the company that there are four activities on which money can be spent to mitigate the occurrence of fraud. These four activities are (1) fraud prevention, (2) early fraud detection, (3) fraud investigation, and (4) follow-up legal action and/or resolution. The consultant would inform the company representatives that there is no such thing as a small fraud—just large frauds that are caught early. The consultant would most likely tell the company that frauds grow geometrically and that, if frauds are allowed to continue unchecked, perpetrators get braver and braver and the amounts stolen or manipulated in the final weeks of the fraud usually dwarf the amounts taken in the early periods of the fraud. The advice

would include a combination of fraud training, ethics programs, better controls, reviewing incentive programs, and harsher treatment of perpetrators. Indeed, a comprehensive fraud program would focus on all four elements of fraud: prevention, proactive detection, investigation, and legal follow-up. Like many organizations, Mark-X has probably been concentrating its fraud-fighting efforts on only the last two: fraud investigation (once the frauds had become so large and egregious that they could no longer be ignored) and follow-up legal action. These are probably the least effective and most expensive fraud-fighting efforts.

An overview of all four elements of a comprehensive fraud program provided in this chapter will help you understand the various fraud-fighting efforts.

Remember this …

There are four fraud-fighting activities that organizations can use: (1) fraud prevention, (2) proactive fraud detection methods, (3) fraud investigation once fraud is suspected, and (4) legal follow-up of fraud perpetrators. Many organizations focus on the last two, which are the most costly and least effective. An overview of these four fraud-fighting activities is given in this chapter.

Fraud Prevention

Preventing fraud is generally the most cost-effective way to reduce losses from fraud.[1] Once a fraud has been committed, there are no winners. Perpetrators lose because they are usually first-time offenders who suffer humiliation and embarrassment as well as legal consequences. They usually must make tax and restitution payments, and there are often financial penalties and other consequences. Victims lose because not only are assets stolen but they also incur legal fees, lost time, negative publicity, and other adverse consequences. Further, if organizations don't deal harshly with the perpetrators, a signal is sent to others in the organization that nothing serious happens to fraud perpetrators, making fraud by others more likely. Organizations and individuals that have proactive fraud prevention measures usually find that their prevention efforts pay big dividends. On the other hand, the investigation of fraud can be very expensive.

STOP & THINK *Why do you think a fraud perpetrator who is caught would suffer more humiliation and embarrassment than a bank robber or other property offender?*

As we explained in Chapter 2, people commit fraud because of a combination of three factors: (1) perceived pressure, (2) perceived opportunity, and (3) some way to rationalize the fraud as acceptable. In Chapter 2, we introduced a scale showing that these factors differ in intensity from fraud to fraud. When perceived pressures and/or opportunities are high, a person needs less rationalization to commit fraud. When perceived pressures and/or opportunities are low, a person needs more rationalization to commit fraud. Unfortunately, sometimes pressures and/or the ability to rationalize are so high that no matter how hard an organization tries to prevent fraud, theft still occurs. Indeed, fraud is generally impossible to prevent completely, especially in a cost-effective way.[2] The best an organization can hope for is to manage the costs of fraud effectively.

Organizations that explicitly consider fraud risks and take proactive steps to create the right kind of environment and reduce its occurrence are successful in preventing most frauds.

Effective **fraud prevention** involves two fundamental activities: (1) taking steps to create and maintain a culture of honesty and high ethics and (2) assessing the risks for fraud and developing concrete responses to mitigate the risks and eliminate the opportunities for fraud. We discuss these activities in the following paragraphs.

Creating a Culture of Honesty and High Ethics

Organizations use several approaches to create a culture of honesty and high ethics. Five of the most critical and common elements are (1) making sure that top management models appropriate behavior, (2) hiring the right kind of employees, (3) communicating expectations throughout the organization and requiring periodic written confirmation of acceptance of those expectations, (4) creating a positive work environment, and (5) developing and maintaining an effective policy for handling fraud when it does occur.

Tone at the Top (Proper Modeling)

Research in moral development strongly suggests that honesty can be best reinforced when a proper example (model) is set—sometimes referred to as the *tone at the top*. Management of an organization cannot act one way and expect others in the organization to behave differently. Management must reinforce to its employees through its actions that dishonest, questionable, or unethical behavior will not be tolerated.[3]

Research into why people lie (or are dishonest) indicates that there are four major reasons why people lie. The first is fear of punishment or adverse consequences. The fear may be because they know they have done something wrong or their performance hasn't met expectations. Individuals who are constantly in fear of being punished develop a habit of lying, which is a second reason for lying. Even when confronted by the truth, once they are conditioned to lie, they usually insist the lie is the truth. A third reason for lying is because they have learned to lie by watching others lie or through negative modeling. When people see others lie, especially when those others get away with their lies, people may become more prone to lying. Finally, people lie because they feel if they tell the truth they won't get what they want.[4]

Unfortunately, bad modeling is everywhere today. And, with increased accessibility to information (blogs, Web sites, PDAs, cable, podcasts, etc.), news about bad modeling is more detailed and more accessible than ever before. So, when someone like Bernie Madoff is alleged to have committed a fraud, his bad modeling is not only known in detail throughout his firm and among his close associates but it is also broadcast through numerous media around the world.

Hiring the Right Kind of Employees

The second key element in creating a culture of honesty and high ethics is hiring the right employees. Not all people are equally honest or have equally well-developed personal codes of ethics. In fact, research results indicate that many people, when faced with significant pressure and opportunity, will behave dishonestly rather than face the "negative consequences" of honest behavior (e.g., losing reputation or esteem, failing to meet quotas or expectations, having inadequate performance exposed, inability to pay debts, etc.). If an organization is to be successful in preventing fraud, it must have effective hiring policies that discriminate between marginal and highly ethical individuals, especially when recruiting for high-risk positions. Proactive hiring procedures include such things as conducting background investigations on prospective employees, thoroughly checking references and learning how to interpret responses to inquiries asked about candidates, and testing for honesty and other attributes.[5]

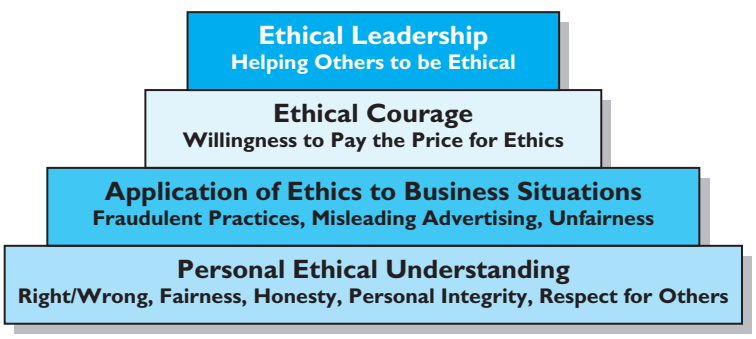
Recent research[6] has suggested an **ethical maturity model (EMM)** (shown in Figure 3.1) that explains why people make unethical decisions.

The foundation of ethics, *Personal Ethical Understanding,* represents the most basic ethical boundaries of personal actions. It involves learning the difference between right and wrong, developing a sense of fair play, learning to care for and empathize with others, developing respect for others, learning basic principles of integrity and reality, and acting in a consistent manner with the values a person knows to be right.

The second level of the EMM, *Application of Ethics to Business Situations,* is being able to translate one's ethical understanding to the business world or to other settings in which people earn a living (e.g., the medical profession, engineering profession, etc.). Such translation is not always easy. For example, a person may have very strong ethics in the way he or she treats family and friends, but may not understand how cooking the books or failing to submit tax withholdings to the government affects peoples' lives or constitutes unethical or fraudulent behavior.

Most of the people involved in the financial shenanigans of the past few years considered themselves

FIGURE 3.1 ETHICS DEVELOPMENT MODEL



to be honest, ethical people. Yet, when faced with decisions about whether to go along with requests to "cook the books" or to reveal observed inappropriate behavior, they made the wrong choices. They did not know how or were afraid to translate their personal ethical values to the business world.

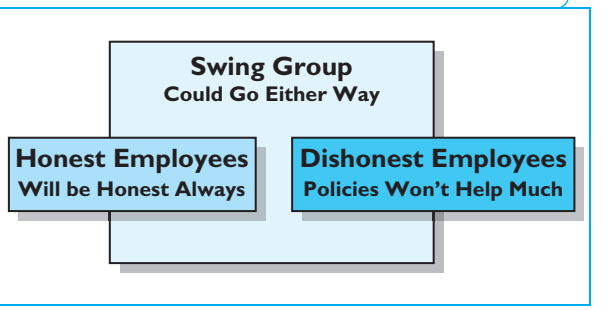
The third level of the EMM is *Ethical Courage*. Ethical courage is the strength and conviction to act appropriately in difficult or questionable situations. A person can have a personal ethical understanding and be able to translate that understanding to business settings but may not have the courage to take a stand when necessary. In one recent fraud, for example, more than 20 people falsified financial statements. All testified they were aware that their actions were unethical, but none had the courage to stand for their beliefs.

The highest level, *Ethical Leadership,* is instilling in others a desire to develop ethical awareness and courage. This higher form of ethical behavior requires a person to inspire others through word, example, persuasion, and good management.[7] We believe the employees in most organizations look something like those shown in Figure 3.2.

In most organizations, there is a small group of employees who have well-defined personal codes of conduct and who have learned how to translate those ethical values to business settings. They also have the courage to do what is right. These employees will almost always do the right thing. There is another small group that lacks strong personal codes of conduct. This group will be dishonest anytime it benefits them. The largest group, however, is the "swing group" comprised of individuals with situational ethics. This group knows what is right and wrong, knows how to translate their ethical values to the business world, and at times even have the courage to do what is right. Yet, because of inconsistent modeling and labeling, their ethics depend upon the situation they are placed in. Generally, this group will follow their leaders and can be influenced by organizational structure and culture. When there is a strong, positive tone at the top and strong ethical leadership in the company, this large group will usually make the right decisions. The labeling and modeling of the leaders sends a powerful message that keeps employees honest and making the right decisions.

Companies should do their best to both hire ethical individuals and then make sure that the right tone at the top is set by executives. Consider the following case of how poor hiring allowed fraud to occur in an organization:

FIGURE 3.2 HONESTY OF EMPLOYEES



Philip Crosby was a former president of ITT. While president, he wrote a book advocating that producing error-free products was possible and could be very profitable. He left ITT to form Philip Crosby Associates, Inc. (PCA), a consulting firm based on his own book's principles. The new company became so successful that it began to attract Fortune 500 executives, who paid large fees to spend a few days at PCA with Philip. PCA was a unique reflection of its founder's values. Crosby argued that to produce error-free products, you have to have an environment of mutual respect. If employees have pride in working for their company, and feel that their company is open and honest, they will perform to the best of their abilities and will not steal from the company. PCA had an international division, created in 1984, that posted $2 million in sales in its first year and had expectations to double that figure in the second year. In February of the second year, PCA opened an office in Brussels and had more offices in the planning stages. PCA decided it needed a director of finance who could work with each new country's reporting rules and translate foreign currencies into their U.S. equivalents. After a reasonable search, the eight senior PCA executives agreed to hire John C. Nelson. John had an M.B.A. and seemed to have an impressive understanding of the technical aspects of the international marketplace. He also had an impressive reference provided to PCA by his previous company. Steve Balash, vice president of human resources, said, "He seemed like the kind of honest individual we'd want to hire." Unfortunately, John C. Nelson was not an honest individual. In fact, he wasn't even John C. Nelson. Rather, his real name was Robert W. Liszewski. When hired, Robert decorated his office with an Illinois CPA license; the CPA certificate had been created on his home computer. The background reference that was provided to PCA had been written by Robert's wife, who was a part-time worker with "John's former employer." Robert's job at PCA was to develop financial information for PCA's fast-growing international operations. Robert's work did not go very smoothly, even from the start. He was terribly slow at converting numbers from foreign currencies to U.S. dollars,

which should not have been a tough task for a CPA. In addition, his monthly reports were always late. After about a year on the job, Robert faced his first big test. The company's third-quarter report deadline had passed, and Robert was far from completing it. His excuses ranged from "The outside bookkeepers … haven't yet computed the final receipts" to "the computer crashed." PCA executives decided to let Robert continue because he seemed to be catching on and was doing better on other projects. In December of the third year, Robert's bookkeeper quit, leaving him completely in charge of all the money that flowed through that division (approximately $12 million that year). Robert quickly became hopelessly behind in keeping the books and was finally called in to explain his problems to the chief financial officer. In the interview, Robert started crying, saying that he had cancer and had only three months to live. The chief financial officer believed Robert's lie, and he was allowed to keep his job. PCA's business began to get worse. In the third year, the company's stock fell to $12 per share from $20 the year before. On March 12 of that year, the chief financial officer tried to move $500,000 from one bank account to another. He was informed by the controller that the account did not have a sufficient balance for the transfer. The CFO knew that the account was supposed to have at least $1 million in it. To see where the money went, the controller scanned the ledgers of wire transfers from the questionable account. She found an unposted transfer that did not appear to be legitimate. The amount of $82,353 had been transferred to a U.S. company called Allied Exports, supposedly to pay for shipping products to Brussels. The materials were being sent from South Bend, Indiana, to Brussels. The controller knew that South Bend was Robert's hometown, but did not think anything of it. Subsequent searches found several more wire transfers to South Bend totaling more than $425,000. The company called the Indiana secretary of state's office to check on Allied Export's incorporation records. They were informed that the president of Allied Export was a woman named Patricia Fox. Management recognized Patricia as Robert's wife. With help from his wife, Robert had created a dummy company in South Bend, Indiana. In over eight months, Robert funneled over $961,000 to the dummy company by charging the expenditures to a number of different expense accounts. Robert's wife was arrested in South Bend when she tried to withdraw $230,000 from the account. In their home, detectives found PCA's ledgers that Robert had stolen and a lockbox that contained all of Allied Export's monthly statements, canceled checks, and incorporation papers. While searching the house, the police spotted Robert driving by in a white Porsche, but they were unable to catch him. Two weeks later, police computers showed a new driver's license had been issued to a John C. Nelson. When they checked out the address, police found an elderly man. The man was the real John C. Nelson, who identified Robert's picture as his old boss, Bruce Fox, who had been fired from a bank in Indiana when the bank discovered that he had previously served an 18-month sentence for embezzling $400,000.

Research on honesty shows that individuals fall into three groups: (1) those who will almost always be honest (approximately 30 percent of the population); (2) those who are situationally honest,[8] who will be honest when it pays to be honest but dishonest when it pays to be dishonest (approximately 40 percent of the population); and (3) those who will always be dishonest (approximately 30 percent of the population). Good modeling and other good fraud prevention measures will usually keep the second group from being dishonest; there is usually not much that can be done to prevent the third group from being dishonest. As a result, having good screening policies in place to eliminate the hiring of dishonest individuals and having positive modeling for situationally honest individuals can prevent most frauds from occurring in an organization. In Chapter 4, we discuss various ways to hire honest employees.

Communicating Expectations of Honesty and Integrity

The third critical element in creating a culture of honesty and high ethics—communicating expectations of honesty and integrity—includes (1) identifying and codifying appropriate values and ethics, (2) fraud awareness training that helps employees understand potential fraud problems they may encounter and how to resolve or report them, and (3) communicating consistent expectations about punishment of violators. For **codes of conduct** to be effective, they must be written and communicated to employees, vendors, and customers.[9] They must also be developed in a manner that will encourage management and employees to take ownership of them.[10] Requiring employees to confirm in writing that they understand the organization's ethics expectations is an effective element of communication in creating a culture of honesty. In fact, many successful organizations have found that annual written confirmation is very effective in both preventing and detecting frauds before they become large.

Red Hat, Inc., a provider of open source software solutions to businesses, has an extensive code of conduct. That code, which is publicly available on Red Hat's website[11] and included in Appendix A of this chapter, shows that all Red Hat employees are required to certify that they will abide by the company's code of conduct.

In addition to expectations about ethical behavior, expectations about punishment of those who commit fraud must also be clearly communicated from top management to everyone in the organization. For example, a clear statement from management that dishonest actions will not be tolerated and that violators will be terminated and prosecuted to the fullest extent of the law is helpful as part of a fraud prevention program. Obviously, such a statement must be followed up with real discipline when fraudulent acts occur.

Codes of conduct (like Red Hat's) are required under the Sarbanes-Oxley Act of 2002 to convey expectations about what is and is not appropriate in an organization. Every public company today must have such a code for its directors and officers.

STOP & THINK *Do you really believe that having a written code of conduct will reduce fraud and other dishonest acts in an organization? Why or why not?*

Creating a Positive Work Environment

The fourth element in creating a culture of honesty and high ethics involves developing a positive work environment. Research results indicate that fraud occurs less frequently when employees have positive feelings about an organization, and have a feeling of ownership in that organization, than when they feel abused, threatened, or ignored. Factors that have been associated with high levels of fraud and that detract from a positive work environment include the following:

1. Top management that does not care about or pay attention to the behavior of employees,
2. Negative feedback or lack of recognition of job performance,
3. Perceived inequities in an organization,
4. Autocratic rather than participative management,
5. Low organizational loyalty,
6. Unreasonable budget expectations,
7. Unrealistically low pay,
8. Poor training and promotion opportunities,
9. High turnover and/or absenteeism,
10. Lack of clear organizational responsibilities, and
11. Poor communication within the organization.

As an indication of the changing nature of companies and how they treat their employees, consider the case of IBM. From the time IBM was organized as Computing Tabulating Recording Company in 1911 until the 1980s, IBM's job security was legendary. It wasn't unusual to find two generations of the same family working for the company. There were never any layoffs or unions. This loyalty to employees buttressed the promise to customers: A happy and motivated workforce meant good service.

However, the bond between the company and its workers began to fray with massive reorganizations in the 1980s, followed by huge layoffs of employees. Like many other companies, IBM's employees felt less job security and ownership in the company.

With today's focus on short-term results, particularly quarterly earnings per share, and the effect those results have on stock prices, many companies have started to treat their employees more like assets that can be bought and sold rather than individuals who need to be nurtured and invested in. With increased layoffs and rehires, comes less security, commitment, and perceived ownership in companies. And, less perceived ownership and commitment to a company often results in an increase in frauds against those companies.

Proper Handling of Fraud and Fraud Perpetrators When Fraud Occurs

The fifth and final element in creating a culture of honesty and high ethics is having appropriate policies in place for handling fraud if it occurs. No matter how good an organization's fraud prevention activities are, as stated previously, fraud can still occur. The way an organization reacts to fraud incidents sends a strong signal that affects the number of future incidents. An effective policy for handling fraud should ensure that the facts are investigated thoroughly, firm and consistent actions are taken against perpetrators, risks and controls are assessed and improved, and communication and training are ongoing. Every organization should have a fraud policy that determines whose responsibility fraud prevention, detection, and investigation are, how incidents of fraud will be handled legally, and what kind of remediation and education efforts will take place when fraud does occur.

Assessing and Mitigating the Risk of Fraud

In addition to creating a culture of honesty and high ethics, effective fraud prevention involves eliminating opportunities for fraud to occur. Neither fraud committed by top management on behalf of an organization, nor fraud committed against an organization can occur without perceived fraud opportunity. Organizations can proactively eliminate fraud opportunities by (1) accurately identifying sources and measuring risks, (2) implementing

appropriate preventative and detective controls to mitigate those risks, (3) creating widespread monitoring by employees, and (4) having internal and external auditors who provide independent checks on performance.

Identifying, sourcing, and measuring the risk of fraud means that an organization should have a process in place that both defines where the greatest fraud risks are and evaluates and tests controls that mitigate those risks. In identifying fraud risks, organizations should consider organizational, industry, and country-specific characteristics that influence the risk of fraud. One organization that effectively prevented most frauds held brainstorming sessions with members of management, internal audit, corporate security, and legal counsel and focused on the following questions:

- *If fraud were to occur in our organization, where would it most likely happen? The types of fraud that were perceived as most likely were cataloged, and the organization paid special attention to these types of fraud.*
- *Which of our employees are in the best positions to commit fraud against our company? The organization then made sure that appropriate preventive and detective controls were in place around those employees.*
- *If each of these possible frauds were to occur in our organization, what kinds of symptoms would they generate?*

Once fraud risk assessment has taken place, the organization can identify the processes, controls, and other procedures that are needed to mitigate the identified risks. An appropriate internal control system will include a well-developed control environment, an effective accounting system, and appropriate control activities. Risks, control environments, and control activities are discussed in Chapter 4.

Research has shown that it is employees and managers, not auditors, who detect most frauds. They are the ones who work side by side with perpetrators and can most easily recognize changes in behavior, lifestyle, financial records, and other things that would indicate that fraud might be occurring. Because coworkers can more easily detect fraud than can auditors and others who provide only episodic reviews, to effectively prevent and detect fraud, employees and managers must be taught how to watch for and recognize fraud. The most effective way to involve employees in the monitoring process is to provide a protocol for communication that informs employees and others to whom they should report suspected fraud and what form that communication should take. The protocol should assure confidentiality and stress that retribution will not be tolerated. Organizations that are serious about fraud prevention must make it easy for employees and others to come forward and must reward and not punish them for doing so.

Remember this …

Fraud prevention involves two elements: (1) creating and maintaining a culture of honesty and high ethics and (2) assessing the risks for fraud and developing concrete responses to mitigate the risks and eliminate the opportunities for fraud. Five of the most critical and common elements in creating a culture of honesty and ethics are (1) making sure top management models appropriate behavior, (2) hiring the right kind of employees, (3) communicating expectations throughout the organization and requiring periodic written confirmation of acceptance of those expectations, (4) creating a positive work environment, and (5) developing and maintaining an effective policy for handling fraud. Organizations can proactively mitigate risks and eliminate fraud opportunities by (1) accurately identifying sources of and measuring risks, (2) implementing appropriate preventative and detective controls to mitigate those risks, (3) creating widespread monitoring by employees, and (4) having internal and external auditors who provide independent checks on performance.

The **Sarbanes-Oxley Act of 2002** recognized the value of having a system for employees and others to report wrongdoing, including fraud. Section 307 of that law requires every public company to both have a whistle-blower system in place and prohibit retaliation against any employee or other person who reports questionable activities using the whistle-blower system. One of the events that prompted this legislation was a letter that former Enron chairman Kenneth Lay received from a senior executive in August 2001 warning that the company—once a pillar of the U.S. energy industry—could "implode in a wave of financial scandals." Apparently, the letter pointed out the questionable nature of some partnerships involving company executives.

The letter was unsigned, but its author was later identified as Sherron Watkins, a vice president for corporate development at Enron. If Enron directors had seen Sherron Watkins's whistle-blowing letter, Enron might still be a going concern, but, unfortunately, she sent her letter to the CEO, not to members of the board or anyone

else. The rest is now history. Congress's response to Enron and other corporate scandals was to place responsibility on a company's audit committee (a subcommittee of the board of directors) to implement and oversee a whistle-blowing process for soliciting, evaluating, and acting on complaints about how the company handles financial reporting and securities law compliance.

The final element in eliminating fraud opportunities is having internal and external auditors who provide periodic audits of financial statements and accounting records. While neither internal auditors nor external auditors are usually specifically trained to detect fraud, their presence provides a major deterrent effect and their audits of books and records often discover frauds, especially when they are large. Research has shown that approximately 20 percent of all frauds are detected by auditors.

Fraud Detection

In a fraud perpetrated by a bank teller, the amounts in the Table 3.1 were taken on the dates noted.

When caught, the teller made the following statement: "I can't believe this fraud went on this long without anyone ever suspecting a thing, especially given the larger and larger amounts."

As you can see, this fraud started very small, with the perpetrator stealing larger and larger amounts as it continued. Not being caught, the perpetrator's confidence in his fraud scheme increased, and he became greedier and greedier. In fact, you will note that, on 7-23, there is a two-week period where fraudulent behavior stopped. The reason for this pause in the perpetrator's dishonest behavior was that auditors came to the branch where he worked. You will also notice that once the auditors left, the perpetrator resumed his fraudulent behavior but only stole small amounts. For a short time, he was testing the system to make sure the auditors hadn't detected him or put processes in place that would reveal his dishonest activity. Once he again had confidence that he wouldn't be caught, he quickly escalated the amounts stolen into hundreds of dollars per day.

While the amounts involved in this fraud are small, the pattern is very typical. Like the one described

TABLE 3.1

DATE	AMOUNT STOLEN						
4-1	*$10*	*5-8*	*$20*	*6-5*	*$50*	*7-16*	*$600*
4-4	*$20*	*5-9*	*$30*	*6-9*	*$30*	*7-23*	*$600*
4-7	*$20*	*5-12*	*$30*	*6-10*	*$40*	*8-4*	*$20*
4-9	*$20*	*5-13*	*$30*	*6-11*	*$30*	*8-8*	*$20*
4-10	*$20*	*5-14*	*$30*	*6-12*	*$50*	*8-11*	*$30*
4-14	*$40*	*5-15*	*$30*	*6-13*	*$50*	*8-14*	*$30*
4-16	*$30*	*5-16*	*$40*	*6-16*	*$50*	*8-19*	*$20*
4-22	*$30*	*5-19*	*$40*	*6-17*	*$50*	*8-22*	*$40*
4-23	*$30*	*5-20*	*$40*	*6-18*	*$30*	*8-26*	*$400*
4-24	*$30*	*5-21*	*$40*	*6-20*	*$70*	*8-27*	*$600*
4-25	*$30*	*5-22*	*$20*	*6-23*	*$100*	*8-28*	*$400*
4-28	*$30*	*5-27*	*$30*	*6-24*	*$200*	*9-2*	*$400*
4-29	*$30*	*5-28*	*$40*	*6-25*	*$400*	*9-5*	*$100*
4-30	*$30*	*5-29*	*$40*	*6-26*	*$600*	*9-12*	*$100*
5-1	*$20*	*5-30*	*$50*	*7-8*	*$400*	*9-15*	*$200*
5-5	*$30*	*6-2*	*$40*	*7-9*	*$700*	*9-16*	*$400*
5-6	*$30*	*6-3*	*$50*	*7-14*	*$400*		
5-7	*$20*	*6-4*	*$50*	*7-15*	*$600*		

previously, most frauds start small and, if not detected, continue to get larger and larger. Events that scare or threaten the perpetrator result in discontinuance of the fraud, only to be resumed when threats pass. Because perpetrators increase the amounts they steal, in most cases, amounts taken during the last few days or months of a fraud far exceed those taken during earlier periods. In one case, for example, the amounts taken quadrupled every month during the period the fraud continued. As stated previously, there are no small frauds—just large ones that are detected early. And, in cases where it is top management or business owners who are perpetrating the fraud, fraud prevention is difficult and early detection is critical. Consider the following fraud:

> *The president of a New Hampshire temporary service company intentionally misclassified employees as independent contractors rather than as employees of his company. The misclassification allowed him to avoid paying $211,201 in payroll taxes over a three-year period. In addition, he provided an insurance company with false information on the number of people he actually employed, thereby avoiding $426,463 in workers' compensation premiums.*

When fraud is committed by the president or owner of an organization, as it was in this case, prevention is very difficult. Maybe the president's company could have had a higher code of ethics, but if the president wants to commit fraud, there is probably nothing anyone can do to stop him. Rather, the emphasis on these types of fraud must be on fraud detection. Because all frauds cannot be prevented, organizations should have both preventive and detective controls in place. Preventive controls are aimed at keeping fraud from happening, while the goal of detective controls is to catch frauds early before they have a chance to get very large.

As a third example of how frauds increase over time, consider the case of a Japanese copper trader who was making rogue trades. Over a period of nine years, his fraudulent trading resulted in a fraud totaling $2.6 billion. The following theft amounts show how much the fraud grew by not being detected early:

YEAR OF FRAUD	CUMULATIVE AMOUNT OF THE FRAUD
Year 1	$600,000
Year 3	$4 million
Year 5	$80 million
Year 7	$600 million
Year 9	$2.6 billion

In years 8 and 9, four of the world's largest banks became involved and lost over $500 million.

The detection of fraud includes steps or actions taken to discover a fraud that has been or is being committed. Detection does not include investigative procedures taken to determine motives, extent, method of embezzlement, or other elements of the dishonest act. As you will discover in subsequent chapters, fraud is unlike other crimes that are easily recognized. Because fraud is rarely obvious, one of the most difficult tasks is determining whether or not a fraud has actually occurred.

Detection of fraud usually begins by identifying symptoms, indicators, or red flags[12] that tend to be associated with fraud. Unfortunately, these "red flags" can often be associated with nonfraud factors as well. There are three primary ways to detect fraud: (1) by chance, (2) by providing ways for people to report suspicions of fraud, and (3) by examining transaction records and documents to determine if there are anomalies that could represent fraud. In the past, most frauds were detected by accident. Unfortunately, by the time detection occurred, the frauds were usually large and had been going on for some time. In most cases, there were even individuals in the victim organizations who suspected that fraud was occurring but did not come forward, either because they weren't sure it was fraud, didn't want to wrongly accuse someone, didn't know how to report the fraud, or were fearful of the consequences of becoming a whistleblower.

In recent years, organizations have implemented a number of initiatives to detect fraud more proactively. The first and most common proactive fraud detection approach has been to install reporting hotlines (**whistle-blowing systems**) as described earlier whereby employees, coworkers, and others can call in using a telephone or submit (using a Web page) an anonymous tip of a suspicion of fraud. Some of these hotlines are maintained within the company, and others are outsourced to independent organizations to provide hotline services for them. (The Association of Certified Fraud Examiners and a company called Allegience [formerly Silent Whistle], for example, provide fee-based hotline service.) Organizations that have installed hotlines have detected many frauds that would have remained undetected, but they have often paid a fairly high price for doing so. Not surprisingly, many of the calls made through hotlines do not involve fraud at all. Some represent nonfraud issues such as employee work-related concerns; some represent hoaxes; some are motivated by grudges, anger, or a desire to do

harm to an organization or an individual; and some represent honest recognition of fraud symptoms that are caused by nonfraud factors.

CAUTION *It is very important that fraud fighters exercise care when proactively detecting fraud. First, there are almost always alternative explanations for what looks like fraud symptoms. For example, a person whose lifestyle suddenly changes could have inherited money from a deceased relative. Second, it is important that proactive fraud detection does not get in the way of effective business. As an example, one of the authors of this book trained several internal auditors of a large corporation how to proactively detect fraud. After a few months, however, those trained auditors had succeeded in upsetting nearly all managers in the company because of their egregious and sometimes disruptive fraud detection techniques. Fraud detection efforts are best when they are invisible to employees and managers of an organization.*

The second proactive fraud detection approach is to analyze data and transactions to look for suspicious trends, numbers, and other anomalies. Recent developments in technology have allowed organizations to comprehensively analyze and mine databases to proactively look for fraud symptoms. Banks, for example, have installed programs to identify suspected kiting. These programs draw the bank's attention to customers who have a high volume of bank transactions within a short period of time. Insurance companies have implemented programs that examine claims within a short time after purchasing insurance. Some organizations have even implemented comprehensive fraud detection programs by systematically identifying the kinds of frauds that could be occurring, cataloging the various symptoms those frauds would generate, and then building real-time queries into their computer systems to search for these symptoms. Fraud detection research, mostly using technology-based search techniques, is now being conducted by academics and other investigators. Anyone who is seriously interested in understanding and fighting fraud should be following this research. In the next two chapters, we will discuss proactive fraud detection.

As an example of proactive **fraud detection**, a large U.S. bank installed a back-room function that used computer programs to scan customer transactions looking for unusual activity. Customers who make rapid deposit and withdrawal transactions, especially depositing checks written on the same account, for example, are often committing the fraud of kiting. Once kiting is suspected, the branch where the suspect's account is domiciled is contacted and told to look into possible fraud. In one instance, the branch was warned that a particular three-year customer had account activity that looked as if he were kiting. Unfortunately, the branch manager knew the customer and felt that he was trustworthy. A few days later, the branch was again notified that this same customer's deposit and withdrawal activity looked very suspicious. Finally, after the third warning, the branch manager decided to investigate. In the meantime, the other bank the dishonest customer was using had discovered the kiting and this bank was left to cover the loss which had grown from $70,000 to over $600,000 between the first and third notification by those doing the data mining. As this real account illustrates, proactive fraud detection can be very valuable, but only when the symptoms generated are not ignored.

Remember this …

Fraud detection involves activities to determine whether or not it is likely that fraud is occurring. Fraud detection allows companies to identify suspicions or predications of fraud. Historically, most frauds were caught by chance. In recent years, two major proactive fraud detection developments have occurred: (1) installing hotlines or whistle-blower systems and encouraging employees and others to report any suspicious activity they see and (2) mining various databases looking for unusual trends, numbers, relationships, or other anomalies that could indicate fraud.

Fraud Investigation

Mark and Jane were husband and wife. Mark was the CEO of McDonald's Incorporated, and Jane was a partner in the CPA firm of Watkiss[13] and McCloy. After a hard day at work, they met at a local restaurant for dinner. Mark told Jane about an incident that happened at work. He showed her an anonymous note that stated: "You had better look into the relationship between John Beasley (the manager of the purchasing department) and the Brigadeer Company (a supplier) because something fishy is going on." He told Jane that he had no idea who sent him the note and that he wasn't even sure what to do about it. He told her that he was concerned about possible collusion and should probably pursue the "lead." Jane couldn't believe what she was

hearing. "What a coincidence," she stated. "Today, something very similar happened to me." She said that a junior auditor had approached her, confiding in her that he was concerned that the client's sales were overstated. He said that he had found some sales contracts without support (there was usually significant documentation supporting the contracts), all signed at the end of the accounting period. He told Jane that he was concerned that the client was artificially inflating revenues to improve the company's financial performance.

Both of these situations involve matters that need to be investigated. If Mark does not investigate the anonymous tip, he may never uncover a possible kickback fraud and inflated purchasing costs for the company. Likewise, Jane needs to perform some follow-up investigation on the revenue problem brought to her attention by the junior auditor.

There are at least three reasons why the auditors in this case must investigate to determine whether or not the client is really overstating revenues. First, the company's shareholders could face significant losses. Second, the auditors' failure to discover the overstatement could expose them to legal action (and consequent losses). Finally, and perhaps most important, an overstatement of revenues may expose management's integrity to such serious doubt as to make the firm "unauditable."

Both of these situations have created a "predication of fraud." **Predication** refers to the circumstances, taken as a whole, that would lead a reasonable, prudent professional to believe a fraud has occurred, is occurring, or will occur. Fraud investigations should not be conducted without predication. A specific allegation of fraud against another party is not necessary, but there must be some reasonable basis for concern that fraud may be occurring. Once predication is present, as in these cases, an investigation is usually undertaken to determine whether or not fraud is actually occurring, as well as the who, why, how, when, and where elements of the fraud. The purpose of an investigation is to find the truth—to determine whether the symptoms observed actually represent fraud or whether they represent unintentional errors or other factors. Fraud investigation is a complex and sensitive matter. If investigations are not properly conducted, the reputations of innocent individuals can be irreparably injured, guilty parties can go undetected and be free to repeat the act, and the offended entity may not have information to use in preventing and detecting similar incidents or in recovering damages.

Approaches to Fraud Investigation

The investigation of fraud symptoms within an organization must have management's approval. Investigations can be quite expensive and should be pursued only when there is reason to believe that fraud has occurred (when predication is present).

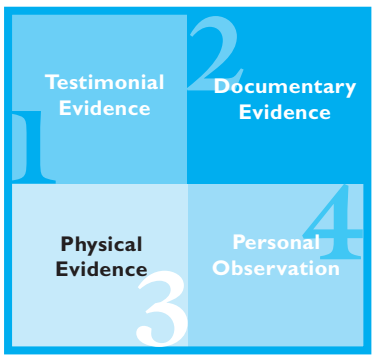
CAUTION *Fraud investigations must be undertaken with extreme care. It is important not to alert potential perpetrators about the investigation, or they can hide or destroy evidence. In addition, since most fraud perpetrators are first-time offenders, the thought of being caught is a traumatic experience for them and there have been many cases where perpetrators have become aware that they were targets of investigation and have committed suicide or taken other drastic actions.*

The approaches to fraud investigation vary, although most investigators rely heavily on interviews. Fraud investigations can be classified according to the types of evidence produced or according to the elements of fraud. Using the first approach, the evidence square in Figure 3.3 shows the four classifications of investigation techniques.

The four types of evidence that can be accumulated in a fraud investigation are as follows:

1. **Testimonial evidence**, which is gathered from individuals. Specific investigative techniques used to gather testimonial evidence are interviewing, interrogation, and honesty tests.
2. **Documentary evidence**, which is gathered from paper, computers, and other written or printed sources. Some of the most common investigative techniques for gathering this evidence include document examination, data mining, public records searches, audits, computer searches, net worth calculations, and financial statement analysis. Recently, corporate databases and e-mail servers have been very useful sources of documentary evidence.
3. **Physical evidence** includes fingerprints, tire marks, weapons, stolen property, identification numbers or marks on stolen objects, and other tangible evidence that can be associated with dishonest acts. The gathering of physical evidence often involves forensic analysis by experts.
4. **Personal observation** involves evidence that is sensed (seen, heard, felt, etc.) by the investigators themselves. Personal observation investigative techniques involve invigilation, surveillance, and covert operations, among others.

FIGURE 3.3 EVIDENCE SQUARE



A second approach to fraud investigation is to focus on the two different fraud triangles: (1) the fraud motivation triangle and (2) the fraud element triangle. These triangles are shown in Figure 3.4.

Investigation involves investigating the various elements of each of these triangles. In focusing on the fraud motivation triangle, investigators search for perceived pressures, perceived opportunities, or rationalizations that others have observed or heard. Focusing on the fraud element triangle is a little more complicated. **Theft act** investigative methods involve efforts to catch the perpetrator(s) in the embezzlement act or to gather information about the actual theft acts. **Concealment** investigative methods involve focusing on records, documents, computer programs and servers, and other places where perpetrators might try to conceal or hide their dishonest acts. **Conversion** investigative methods involve searching for ways in which perpetrators have spent or used their stolen assets.

Conducting a Fraud Investigation

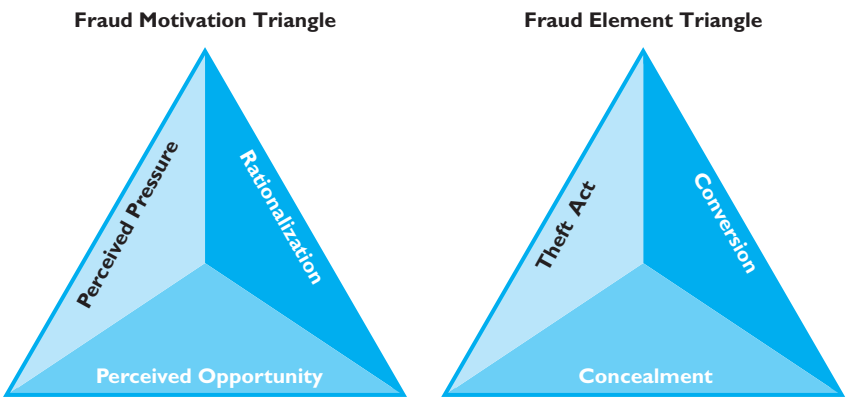
For now, it is important to know that a fraud investigator needs some way to coordinate the fraud investigation. Some investigations are extremely large, and conducting the various investigative steps in the wrong order or doing them inappropriately can lead to a failed investigation as well as other problems. As a result, it is very important to understand the significant risks that investigators face.

And, as stated in the previous caution box, you must also remember that investigating a fraud is a traumatic experience for everyone involved, including the perpetrators. Most fraud perpetrators have positive reputations in their work, community, family, and church environments. Sometimes, admitting that they are being investigated for fraud or have committed fraud is more than they can take. Consider the following obituary, for example:

> *Memorial services for John Jones will be held Thursday, May 5, 2001, at the Springer-Wilson Funeral Home. John was 35 at the time of his death. He was preceded in death by his mother, Jane Jones, and a younger brother, Tom Jones. John is survived by his wife, Rebecca, and four children ages 9, 7, 6, and 4. He is also survived by three brothers, a sister, and his father. In lieu of flowers, please make contributions to the Improvement Memorial Fund for Children.*

This obituary, which is real but has been modified slightly, is for a person who embezzled $650,000 from

FIGURE 3.4 ELEMENTS OF FRAUD



his employer's company. Over a seven-year period, he embezzled nearly half of all cash received from customers. He did not steal when customers used checks or credit cards to pay their bills—only when payment was with cash. When the company finally determined that he was stealing, they called him on the telephone at night and asked him to meet with the company's lawyers the next morning. John did two things that night after receiving the telephone call. First, he called an attorney and told her that he had been stealing from his employer for seven years and would like her to represent him at a meeting with the company's attorneys the next morning. Then, a couple of hours later, he changed his mind, drove into some nearby mountains, and committed suicide.

This actual case illustrates one reason why investigations must be conducted carefully. Maintaining high ethics in conducting investigations is also very important. At a minimum, investigations of fraud must proceed as follows:

1. They must be undertaken only to "establish the truth of a matter under question."
2. The individuals charged with the responsibility for conducting the investigation must be experienced and objective. If individuals conducting investigations do not exercise care in choosing words describing the incident or maintaining a neutral perspective, their objectivity can immediately become suspect in the eyes of management and employees. Investigators should never jump to conclusions.
3. Any hypothesis investigators have about whether or not someone committed fraud should be closely guarded when discussing the progress of an investigation with others. While good investigators often form preliminary opinions or impressions at the start of an investigation, they must objectively weigh every bit of information against known facts and evidence and must always protect the confidentiality of the investigation.
4. Investigators must ensure that only those who have a need to know (e.g., management) are kept apprised of investigation activities and agree to the investigation and techniques employed.
5. Good investigators must ensure that all information collected during an inquiry is independently corroborated and determined to be factually correct. Failure to corroborate evidence is often a key mistake made by inexperienced investigators.
6. Investigators must exercise care to avoid questionable investigative techniques. Experienced investigators make sure that any technique used is scientifically and legally sound and fair. Usually, thoroughness and dogged tenacity rather than questionable techniques lead to a successful investigation.
7. Investigators must report all facts fairly and objectively. Communications throughout the term of an investigation, from its preliminary stage to the final report, should be carefully controlled to avoid obscuring facts and opinions. Communication, including investigative reports, must not only include information obtained that points to guilt, but must also include facts and information that may exonerate. Ignoring and failing to document information is a serious investigative flaw, with potential for serious consequences.

Remember this …

Fraud investigation should only occur when fraud predication exists. The purpose of an investigation is to find the truth—to determine whether the symptoms observed actually represent fraud or whether they represent unintentional errors or other phenomena. There are many different ways to organize and think about fraud investigations including focusing on the types of evidence gathered and the fraud motivation and fraud element triangles. Because of the sensitive nature of fraud investigations, fraud investigators must exercise extreme care in how investigations are conducted, who knows about the investigations, and the way investigations are described.

Follow-Up Legal Action

One of the major decisions a company, stockholders, or others must make when fraud is committed is what kind of follow-up legal and other actions should be taken. Why the fraud occurred should always be determined, and controls or other measures to prevent or deter its reoccurrence should be implemented. Training of appropriate people so that similar frauds won't reoccur is also required. The bigger question that must be addressed, however, is what, if any, legal action should be taken with respect to the perpetrators.

Most organizations and other fraud victims usually make one of three choices: (1) take no legal action, (2) pursue civil remedies, and/or (3) pursue criminal action against the perpetrators, which is sometimes done for them by law enforcement agencies. While

we have already addressed civil and criminal law in Chapter 1 and will discuss follow-up action in future chapters, we will briefly review some of the pros and cons of each alternative here.

Descriptive fraud research has consistently shown that legal action is taken against perpetrators who commit fraud against organizations in less than half of fraud cases. Management often only wants to get the fraud behind it as quickly as possible. It understands that pursuing legal action is expensive, time consuming, sometimes embarrassing, and often considered an unproductive use of time. Most often, management terminates fraud perpetrators, but sometimes it does not even do that. Unfortunately, when organizations do not pursue legal action, the word usually spreads quickly throughout the organization that "nothing serious will happen if you steal from the company." Employees who understand this message are more likely to steal than are employees of organizations who understand that there is an expectation of strict and universal punishment for dishonest acts. When one Fortune 500 company changed its stance on fraud from "the CEO is to be informed when someone is prosecuted for fraud" to "the CEO is to be informed when someone who commits fraud is not prosecuted," the number of frauds in the company decreased significantly.

Civil Action

As you learned in Chapter 1, the purpose of a civil action is to recover money or other assets from the fraud perpetrators and others associated with the fraud. Unless perpetrators have considerable assets (e.g., homes, expensive cars, and other assets), civil actions are quite rare in cases of employee fraud because perpetrators have usually spent the money they stole. However, civil action is much more common when frauds involve other organizations. Vendors who pay kickbacks to company employees are often the target of civil actions by victim companies, especially if the losses to the company are high. Consider the example in the following real case where the names have been changed.

Mark L. was the purchasing agent for a company that purchased large amounts of uniforms for its employees. Mark typically used three different vendors but started accepting bribes from a particular vendor from Korea. Once the bribes were being paid, the control of purchasing transactions shifted from the buyer to the supplier, with the supplier demanding that Mark's company purchase more uniforms at higher prices and even at lower quality. Once the quality deteriorated, the uniforms starting falling apart, changing colors when being washed, and buttons started falling off. In the meantime, the Korean company shifted manufacturing to a lower-cost country and demanded that the purchasing company buy increasing numbers of uniforms. Because of the decreased quality, Mark's company sued the supplier for failing to meet contract specifications. After subpoenaing purchasing records, Mark's company found a 1099 (tax form indicating payment) to Mark. Seeing the red flag that their own purchasing agent was being paid by a supplier, Mark's company hired a fraud examiner who detected and investigated the fraud. Mark's company sued the Korean manufacturer civilly for triple damages according to RICO statues. Just before the trial started, the Korean company settled with Mark's company by paying it $46 million to cover the triple damages and legal fees incurred.

Similarly, stockholders and creditors who suffer losses when management fraud occurs almost always sue not only the perpetrators but also usually the auditors and any others associated with the company who may have "deep pockets." The plaintiff's lawyers are usually more than willing to represent shareholders in class action, contingent fee lawsuits.[14]

Criminal Action

Criminal action can only be brought by law enforcement or statutory agencies. Organizations that want to pursue criminal action against perpetrators must work with local, state, or federal agencies to get their employees or other perpetrators prosecuted. As you learned in Chapter 1, criminal penalties usually involve fines, prison terms, or both. They can also involve the perpetrators entering into restitution agreements to pay back stolen funds over a period of time. Pursuing criminal penalties is becoming more and more common in fraud cases. Corporate executives who commit fraud are often sentenced for up to 10 years in jail and ordered to pay fines equal to the amounts they embezzled.

As an example of criminal penalties that can be imposed, consider the case of Bernie Ebbers, the former CEO of WorldCom.

One of the largest criminal sentences ever handed to a fraud perpetrator was given to ex-WorldCom chief executive Bernie Ebbers in 2005. The 63-year-old Mr. Ebbers was sentenced to 25 years in prison for his role in orchestrating the biggest corporate fraud in U.S. history.

Mr. Ebbers was convicted in March 2005 for his part in the $11 billion accounting fraud at WorldCom that was the

biggest in a wave of corporate scandals at Enron, Adelphia, and other companies.

WorldCom, now known as MCI, filed the largest bankruptcy in U.S. history in 2002. The company's collapse led to billions of dollars in losses for shareholders and employees.

Mr. Ebbers had previously agreed to forfeit the bulk of his assets—including a Mississippi mansion and other holdings estimated to be worth as much as $45 million—to burned WorldCom investors and MCI. His wife did keep a modest home in Jackson, Mississippi, and about $50,000.

Mr. Ebbers appealed the verdict, but it was reaffirmed by a higher court in September 2006.

Remember, however, that it is much more difficult to get a criminal conviction than it is to get a judgment in a civil case. Whereas only a preponderance of the evidence (more than 50 percent) is necessary to win a civil case, convictions are only successful if there is proof "beyond a reasonable doubt" that the perpetrator "intentionally" stole money or other assets.

Remember this …

Once a fraud has been investigated, victim organizations must decide what legal and other actions to pursue. At a minimum, they should make sure that controls are implemented and training takes place to prevent similar occurrences in the future. In addition, the company must decide whether to sue civilly (to try to recover stolen funds) or to pursue criminal prosecution or both. Guilty verdicts in criminal cases can result in prison sentences and/or restitution.

Review of the Learning Objectives

- **Become familiar with the different ways that organizations fight fraud.** Organizations generally fight fraud in four ways: (1) by trying to prevent frauds from occurring, (2) by using proactive detection methods for frauds that do occur, (3) by investigating fraud once there is suspicion (predication) that a fraud is or has occurred, and (4) by following up legally and in other ways.
- **Understand the importance of fraud prevention.** Fraud prevention is the most cost-effective fraud-fighting activity. Once fraud occurs, everyone loses. Fraud prevention involves (1) taking steps to create and maintain a culture of honesty and high ethics and (2) assessing the risks for fraud and developing concrete responses to mitigate the risks and eliminate the opportunities for fraud.
- **Understand how to create a culture of honesty and high ethics.** Organizations that take proactive steps to create a culture of honesty and high ethics can successfully eliminate much fraud. Creating a culture of honesty and high ethics includes (1) making sure that top management models appropriate behavior, (2) hiring the right kind of employees, (3) communicating expectations throughout the organization, (4) creating a positive work environment, and (5) developing and maintaining an effective policy for handling fraud when it does occur.
- **Understand why hiring the right kind of employees can greatly reduce the risk of fraud.** Unfortunately, not all people are equally honest or have equally well-developed personal codes of ethics. If an organization is to be successful in preventing fraud, it must have effective hiring policies that discriminate between marginal and highly ethical individuals, especially when recruiting for high-risk positions. Proactive hiring procedures include such things as conducting background investigations on prospective employees, thoroughly checking references and learning how to interpret responses to inquiries asked about candidates, and testing for honesty and other attributes.
- **Understand how to assess and mitigate the risk of fraud.** Assessing and mitigating the risk of fraud means that an organization should have a process in place that both defines where the greatest fraud risks are and evaluates and tests controls that mitigate those risks. In identifying fraud risks, organizations should consider organizational, industry, and country-specific characteristics that influence the risk of fraud.
- **Understand the importance of early fraud detection.** No matter how good a company's fraud prevention activities are, some frauds will still occur. Companies should use proactive fraud detection techniques, such as whistle-blower systems and data mining tools, to detect frauds before they become large.
- **Understand different approaches to fraud investigation.** Fraud investigation involves the steps taken, once fraud is detected or suspected, to determine the who, why, when, and how much of the fraud. Fraud investigation identifies perpetrators,

amounts taken, and breakdowns in controls or other elements that allowed the fraud to occur. Fraud investigation is expensive and time consuming.

- **Be familiar with the different options for legal action that can be taken once fraud has occurred.** Once frauds occur, companies should take both internal and external actions. Internal actions involve making sure controls and training are in place to prevent future occurrences of similar frauds. External actions include civil suits and/or criminal prosecution.

KEY TERMS

fraud prevention, p. 71
ethical maturity model (EMM), p. 72
codes of conduct, p. 74
Sarbanes-Oxley Act of 2002, p. 76
whistle-blowing systems, p. 78
fraud detection, p. 79
predication, p. 80
testimonial evidence, p. 80
documentary evidence, p. 80
physical evidence, p. 80
personal observation, p. 80
investigation, p. 81
theft act, p. 81
concealment, p. 81
conversion, p. 81

QUESTIONS

Discussion Questions

1. Why is fraud prevention so important?
2. How does building a culture of honesty and high ethics help to reduce the possibility of fraud?
3. How does a company assess and mitigate the risk of fraud within an organization?
4. Why is it important to detect fraud early?
5. Why is it important to conduct a thorough fraud investigation when fraud is suspected?
6. Describe the evidence square.
7. How is the evidence square useful in thinking about fraud investigation?
8. For each of the following, identify whether the evidence would be classified as testimonial evidence, documentary evidence, physical evidence, or personal observation.
   a. Surveillance
   b. Tire marks
   c. Honesty test
   d. Interview
   e. A computer hard drive
   f. A financial statement analysis
   g. A paper report
   h. Identification numbers on vehicles
   i. Audit of financial statements
   j. Check stubs
   k. Fingerprints
   l. Background checks
   m. Interview
9. What are some of the legal actions that can be taken after a fraud has occurred?
10. Why might civil proceeding be ineffective against employee fraud? When might they be more useful?
11. Why might management avoid taking legal action against fraud perpetrators? What are the perceived benefits of inaction? What are the costs?

True/False

1. Once fraud has been committed, there are no winners.
2. Fraud prevention involves two fundamental activities: (1) a hotline for tips and (2) assessing the risk of fraud and developing concrete responses to mitigate the risks and eliminate opportunities for fraud.
3. Developing a positive work environment is of little importance when creating a culture of honesty.
4. No matter how well an organization has developed a culture of honesty and high ethics, most organizations will still have some fraud.
5. Research has shown that it is employees and managers, not auditors, who detect most frauds.
6. Organizations that want to prevent fraud must make it easy for employees and others to report suspicious activities.
7. If a perpetrator is not caught, his confidence in the scheme will decrease, and he will become less and less greedy.
8. Once predication is present, an investigation is usually undertaken to determine whether or not fraud is actually occurring.
9. Most investigators rely heavily on interviews to obtain the truth.
10. Physical evidence includes evidence gathered from paper, computers, and other written documents.
11. Legal action taken by an organization can affect the probability of whether fraud will reoccur.
12. Investigating fraud is the most cost-effective way to reduce losses from fraud.

13. Fraud prevention includes taking steps to create and maintain a culture of honesty and high ethics.
14. Effective hiring policies that discriminate between marginal and highly ethical individuals contribute to an organization's success in preventing fraud.
15. Expectations about punishment must be communicated randomly among work groups if fraud is to be prevented.
16. Frauds typically start large and get smaller as the perpetrator tries to conceal his dishonest acts.
17. Fraud is difficult to detect because some fraud symptoms often cannot be differentiated from nonfraud factors that appear to be symptoms.
18. The three elements of the fraud triangle by which the investigative techniques are often classified are (1) the theft act, (2) concealment efforts, and (3) conversion methods.
19. Organizations often want to avoid embarrassment and expense, so they terminate fraudulent employees without having them prosecuted further.
20. Criminal conviction is much more difficult to achieve than a civil judgment because there must be proof "beyond a reasonable doubt" that the perpetrator intentionally stole assets.
21. In order to create a culture of honesty and confidentiality, persons aware of fraudulent activity should be encouraged to tell only the CEO.
22. Since complete fraud prevention is impossible because it requires changing actual human behavior, successful companies should forgo fraud prevention and instead focus on strong fraud detection programs.
23. Since fraud prevention programs are so costly, despite being ethically superior, they almost always result in higher costs and thus lower net income than using only a strong system of fraud detection.
24. Most fraud perpetrators have a long history of dishonesty and deceit.

Multiple Choice

1. The most effective way to reduce losses from fraud is:
   a. Detecting fraud early.
   b. Implementing proactive fraud detection programs.
   c. Preventing fraud from occurring.
   d. Severely punishing fraud perpetrators.
2. To successfully prevent fraud, an organization must:
   a. Identify internal control weaknesses.
   b. Explicitly consider fraud risks.
   c. Take proactive steps to create the right kind of environment.
   d. All of the above.
3. The best way for management to model appropriate behavior is to:
   a. Enforce a strict code of ethics.
   b. Set an example of appropriate behavior.
   c. Train employees about appropriate behavior.
   d. Make employees read and sign a code of conduct.
4. Which of the following is *not* a proactive way for a company to eliminate fraud opportunities?
   a. Severely punishing fraud perpetrators.
   b. Assessing risks.
   c. Implementing appropriate preventive and detective controls.
   d. Creating widespread monitoring of employees.
5. Most frauds start small and:
   a. If not detected, continue to get larger.
   b. Usually decrease in amount.
   c. Remain steady and consistent.
   d. None of the above.
6. It is most difficult to prevent which type of fraud?
   a. Investment scams.
   b. Fraud committed by a company president.
   c. Employee fraud.
   d. Customer fraud.
7. Which of the following refers to the circumstances, taken as a whole, that would lead a reasonable prudent professional to believe fraud has occurred, is occurring, or will occur?
   a. Evidential circumstance.
   b. Investigation.
   c. Service of process.
   d. Predication.
8. An investigative approach that includes testimonial evidence, documentary evidence, physical evidence, and personal observations is referred to as the:
   a. Investigative square of evidence.
   b. Investigation square.
   c. Evidence square.
   d. Fraud triangle plus.
9. Usually, for everyone involved—especially victims—the investigation of fraud is very:
   a. Pleasant and relaxing.
   b. Educational.
   c. Exciting.
   d. Traumatic and difficult.

10. To prevent fraud from reoccurring, most organizations and other fraud victims should:
    a. Take no legal action.
    b. Pursue civil remedies.
    c. Pursue criminal remedies.
    d. Pursue either civil or criminal action.
11. All of the following are ways to create a culture of honesty and high ethics except:
    a. Creating a positive work environment.
    b. Hiring the right kind of employees.
    c. Having top management model appropriate behavior.
    d. Eliminating opportunities for fraud.
12. The *tone at the top* when related to fraud usually refers to management's attitude about:
    a. Office parties.
    b. Fraud prosecution.
    c. Employee absenteeism.
    d. How it models and labels appropriate behavior.
13. Research shows that fraud occurs less frequently when employees feel:
    a. Abused by management.
    b. Threatened.
    c. Challenged with unreasonable performance goals.
    d. Ownership in the organization.
14. Opportunities to commit fraud can be eliminated by identifying sources of fraud, by implementing controls, and through independent checks. One other effective way of eliminating opportunities is:
    a. Teaching employees to monitor and report fraud.
    b. Terminating and punishing employees who commit fraud.
    c. Failing to terminate or punish employees who commit fraud.
    d. Identifying indicators of fraud or red flags.
15. Drawbacks to establishing a hotline for employees to report fraud include all of the following except:
    a. Expense.
    b. Many incidents reported are hoaxes motivated by grudges.
    c. Fraud symptoms reported are caused by nonfraud factors.
    d. This method for finding fraud is outdated.
16. "Predication of fraud" is defined as:
    a. Reasonable belief that fraud has occurred.
    b. Irrefutable evidence that fraud has been committed.
    c. Motivation for committing fraud.
    d. Punishment of fraud perpetrators.
17. Which of the four types of evidence includes interrogation and honesty testing?
    a. Testimonial.
    b. Documentary.
    c. Physical.
    d. Personal observation.
18. The three elements of fraud are:
    a. Theft act, rationalization, and opportunity.
    b. Pressure, opportunity, and conversion.
    c. Theft act, concealment, and conversion.
    d. Theft act, pressure, and opportunity.
19. Most often, victims of fraud do not take legal action against perpetrators. This is because legal action can be:
    a. Unproductive.
    b. Embarrassing.
    c. Expensive.
    d. All of the above.
20. Arguments for taking legal action against perpetrators of fraud include:
    a. Huge cash settlements from prosecuting fraud are an excellent source of revenue.
    b. Legal action usually results in positive publicity for the company.
    c. Prosecution keeps lawyers busy.
    d. Prosecution discourages reoccurrence of fraud.
21. Factors that are usually associated with high levels of employee fraud include all of the following except:
    a. Negative feedback and lack of recognition of job performance.
    b. Perceived inequalities in an organization.
    c. Long and difficult hours shared equally by everyone in the organization.
    d. High turnover and absenteeism.
22. Which of the following is true regarding the Sarbanes-Oxley Act of 2002:
    a. Companies with revenues exceeding $10 million must have a whistle-blower system in place.
    b. Public companies must have a whistle-blower system in place.
    c. Public companies with revenues exceeding $10 million must have a whistle-blower system in place.
    d. All companies must have a whistle-blower system in place.

SHORT CASES

Case 1

Assume that you are a consultant for Long Range Builders, a company that specializes in the mass production of wood trusses. The trusses are used in the building of houses throughout the United States, Canada, and Mexico. While implementing a fraud prevention program, you realize the importance of creating a culture of honesty and high ethics within the company.

1. What critical elements are key factors in creating an atmosphere of honesty and high ethics?
2. How would you implement these elements in your company?

Case 2

The chapter stressed that preventing fraud is the most cost-effective way to reduce losses from fraud. Why is fraud prevention more cost-effective than fraud detection or investigation?

Case 3

Fraud detection is an important element of minimizing losses to fraud, especially if frauds can be detected early. Explain why it is important that frauds be detected early.

Case 4

Assume that you are the fraud expert for a large Fortune 500 company located in Miami, Florida. In a recent meeting with the executive committee, one of the officers explains that the fraud prevention program, which teaches managers and employees how to detect and report fraud, costs the company $150,000 a year. The officer then explains that it is a waste of time and money for the company to educate employees and managers about fraud. "Is it not the responsibility of the auditors to detect fraud?" he questions. As the fraud expert of the company, the president asks you to explain why managers and employees should be educated in the detection of fraud.

1. What would you tell the committee about why it is important to train managers and employees in fraud detection?
2. After explaining to the committee why it is important to train management and employees, the president asks you about effective ways to involve employees and managers in the prevention and detection of fraud. What would you tell the president?

Case 5

You have recently graduated from college with an MBA. Upon graduation, you start working for Roosevelt Power Plant. The boss, Mr. Jones, invites you into his office. Mr. Jones describes to you a large fraud that has recently taken place in the company. He asks you what actions should be taken to ensure that fraud does not occur again. After analyzing the company, you compile a list of actions that will be needed to prevent fraud from occurring again. Upon presenting the necessary steps and controls to be taken, Mr. Jones notices your suggestion: "Create a culture of honesty and create a positive work environment for employees." Mr. Jones is enraged and wants to know what a positive work environment has to do with the prevention and detection of fraud.

1. What would you tell Mr. Jones about why a positive work environment will help prevent fraud?
2. What factors would you tell Mr. Jones contribute to a negative work environment?

Case 6

The text pointed out that it is important to hire employees who are honest and have a well-developed personal code of ethics. Derek Bok, former law professor and president of Harvard University, has suggested that colleges and universities have a special obligation to train students to be more thoughtful and perceptive about moral and ethical issues. Other individuals have concluded that it is not possible to "teach" ethics. What do you think? Can ethics be taught? If you agree that colleges and universities can teach ethics, how might the ethical dimensions of business be taught to students?

Case 7

Predication refers to circumstances that would lead a reasonable professional to believe that fraud has occurred. Why should you not conduct a fraud investigation without predication?

Case 8

When a fraud has occurred within an organization, management must decide what follow-up action to take. Briefly describe the three follow-up alternatives available to organizations.

Case 9

In 2001, the country of Peru was thrown into political turmoil as its president, Alberto Fujimori, was accused of conspiring with the head of the national army to accept bribes and steal money from the government. As a result, Fujimori fled the country to avoid impeachment and prosecution. Fujimori was elected 10 years earlier based on his promises to lower inflation and combat terrorism. He was not, however, elected for his

honesty. At the time he was elected, many people expressed the thought, "All of our presidents steal from us, but he steals the least." Although he was successful as a president, what could the Peruvian people have done to avoid the frauds committed by President Fujimori?

Case 10

You are the controller at a start-up company named HyperGlobal created by your friend, Kevin. Your company is growing quickly, and you and Kevin are finding it difficult to hire qualified people fast enough. Kevin suggests over lunch that you should expedite the process by skipping the sometimes time-consuming chore of running background checks. He notes, "I interview them anyway, and I can tell if they are honest just by talking to them. We should do away with this silly background checking business." Do you agree? How would you respond to Kevin? What is at stake if hiring mistakes are made?

Case 11

Business 2.0 recently reported on Men's Warehouse's CEO George Zimmer's policy "that no employee or interviewee will ever undergo a criminal background check."[15] The company, however, loses an average of 0.4 percent of revenues to theft, compared to a typical 1.5 percent faced by most large retailers. What things might create this low rate of theft despite not performing criminal background checks?

Case 12

According to the text, when one Fortune 500 company changed its stance on fraud from "the CEO is to be informed when someone is prosecuted for fraud" to "the CEO is to be informed when someone who commits fraud is not prosecuted," the number of frauds in the company decreased significantly. Why might that be?

Case 13

As a fraud expert asked to investigate possible fraud at a local nonprofit organization, you suspect that one of the workers, Stacey, has been embezzling money. After securing enough evidence to be very confident of Stacey's guilt, you speak with the president of the organization, Jamie. Jamie assures you that Stacey could be doing nothing wrong, that she has known Stacey for years, and that Stacey is a good person. Further, she indicates that because of her relationship with Stacey, even if something were going wrong, no action would be taken with respect to the potential fraud. How do you respond to Jamie? How do you explain to her what is at stake?

Case 14

Peter Jones, a senior accountant, and Mary Miller, a junior accountant, were the only accountants for XYZ Company, a medium-size business. Peter had been with the company for over four years and was responsible for the Purchasing Department. Mary had been working at the company for a little over five years, and she had neither applied for a vacation nor taken any days off in the last three years. She was responsible for cash receipts and disbursements. She also collected the cash from the cash register, counted it and matched it with cash register receipts, made a record of daily receipts, and then put the money in the safe. Once a week, she would take the paperwork to her supervisor, Susan Lowe, one of the managers, who would check it. Mary later resigned from the company. At the time of her resignation, Peter was asked to handle Mary's responsibilities while the company looked for a person to replace her. Peter soon realized that there had been some manipulation of accounting records and embezzlement of funds. Investigations revealed that approximately $30,000 had been stolen.

1. What do you think might have allowed this fraud?
2. How could this fraud have been avoided?

CASE STUDIES

Case Study 1

Plutonium was an Internet start-up company founded in 1988 at the beginning of the technology boom. One of the largest problems for Plutonium was developing the technological systems necessary to support the rapidly expanding user base. Furthermore, due to the rapid expansion in recent years, many of its systems had been added hastily, resulting in poor integration and eroding data integrity. As a result, the CEO of Plutonium announced an initiative to integrate all systems and increase the quality of internal data. In compliance with this initiative, Plutonium purchased an expensive and complex billing system called Gateway, which would automate the billing for thousands of Internet accounts via credit cards. During the integration, Gateway, in collaboration with Visa, created a phony credit card number that could be used by developers and programmers to test the functionality and integration of the Gateway system. Moreover, this credit card number was fully functional in "live" environments so testers and developers could ensure functionality without being required to use actual personal or company credit card

numbers (the activity on this card was not monitored). The integration went smoothly; however, it created thousands of corrupt accounts that required fixing.

Jonathan, the manager of the Operations Department, was responsible for the resolution of all data integrity issues. His team was tasked with fixing all corrupt accounts created by the launch and integration of the Gateway system. As a result, Jonathan was given the phony credit card number, which was kept on a Post-it Note in his drawer.

One of the top performers on the Operations team was a 29-year-old male named Chris. Chris had worked in Operations for over a year and was making $15 per hour, the same salary at which he was hired. He was an introvert working to support a family and put himself through school. Chris was the most technologically savvy individual on the team, and his overall systems knowledge even exceeded that of his manager, Jonathon. Chris was very brilliant in creating more efficient tools and methods to repair corrupted accounts. Therefore, Chris was tasked with conducting training for new employees and updating team members on new processes and tools that he had created. As a result, Chris quickly became a trusted and valuable team member; thus, Jonathon gave him and other team members the phony credit card number in order to further increase the productivity of the team.

However, after six months of working at Plutonium, Chris received an official reprimand from the company for using the company system to access Web sites containing pirated software and music. The FBI attended the investigation and determined that Chris had not been a major player in the piracy. Therefore, Chris was quietly warned and placed on a short-term probation. Jonathon was asked to write a warning letter for the action; however, after a brief conversation with Chris, Jonathon determined that Chris's intentions were good and never officially submitted the letter because Chris was a trusted employee and elevated the overall performance of the team. A few months after the piracy incident, Jonathon noticed some changes in Chris's behavior such as (a) his computer monitor was repositioned so that his screen was not visible to other coworkers, (b) he had almost all the latest technological innovations (new Palm Pilot, MP3 player, Play Station, new laptop, and a new car stereo system), (c) he was going out to lunch more frequently, and (d) he frequently used multiple fake usernames and passwords for testing purposes.

Questions

1. Evaluate this case using the three elements of the fraud triangle to identify the following:
   a. Potential pressures for Chris to commit fraud.
   b. Potential opportunities for Chris to commit fraud.
   c. Potential rationalizations that Chris could use to commit fraud.
2. What are some of the symptoms that fraud potentially exists in this situation?
3. What could Jonathon have done to eliminate some of the opportunities for fraud?

Case Study 2

Derek worked for a reputable global consulting firm. His firm specialized in helping companies analyze their people, processes, systems, and strategy. Derek was hired into the San Francisco office and put through weeks of training to help him understand the firm methodology, technology, and culture. The firm looked for people with the right aptitude who had demonstrated a record of success in previous school, work, or extracurricular activities. They found that this type of person worked out best for the type of work the firm was paid to do.

Derek was flattered to be considered the right type of person for this company. He was excited to be assigned to a project and begin work. Even though Derek was trained in certain technologies, he was assigned a project for which he had no training. The project was implementing SAP—a multimillion-dollar enterprise resource planning software package. The client was a mid-sized manufacturer with revenues of approximately $100 million located in Topeka, Kansas.

Derek was not trained in SAP and found out that he was replacing two managers who were just removed from the project. The project was running over budget so the firm looked for ways to get the work done less expensively. Derek, who billed out at the lower "consultant's" rate (instead of the "manager" rate), was a cheap solution, although it would be a tough sell to the client. They liked the previous managers and felt comfortable with their skill level. Because of the demand for the SAP experts, Derek's firm could charge Derek's time at a billing rate of $200/hour—expensive, but less than the client was paying for the managers.

During the first day on the job, Derek's manager took him out to lunch to give him "the scoop" on

what was happening on the project and what he would be expecting from Derek. "Derek, this is going to be a very difficult assignment. You've replaced two skilled managers who the client liked. I know you haven't been trained on, or actually even seen SAP before, but you're smart and can come up to speed quickly. I had to tell the client you were an expert in the software in order for them to agree to bring you on. If you have any questions, don't hesitate to ask me but definitely don't look stupid or seem like you don't know what you're doing in front of the client. The client will be skeptical of you at first, but be confident and you'll win them over. I think the transition will smooth out quickly. See me if you have any questions."

Derek was scared to death—but what was he to do? Was this standard procedure to throw employees into this kind of situation? Regardless, he had to get to work. His immediate tasks were to map out the processes for the client's order-to-cash, purchase-to-pay, and capital acquisition business scenarios. This involved interviewing managers and looking around most of the functional departments in the company. Here are some interesting things he found as he did his work.

PURCHASING DEPARTMENT: The head of purchasing was a handsome gentleman named Mike. Mike was very different from any other employee who Derek encountered while at the client. He wore expensive suits to work and liked to talk about his clothes with colleagues. He also drove the latest model BMW and would take the other consultants on the project for rides during lunch. Derek thought this odd because he didn't think a purchasing manger at this company made enough money to have these luxuries. Mike also took his relationships with "his" vendors very seriously. He would spend lots of time "understanding who they were." Some days, Mike was very supportive of Derek and other days seemed completely different and almost hostile and combative. When Derek informally inquired about the purchasing manager's clothes and car and his Dr. Jekyll and Mr. Hyde syndrome, he heard the following justification, "He probably has a lot of money because he's worked here for over 20 years. Plus, he never takes vacations. Come to think of it, the vacation part probably explains why he seems hostile to you some of the time." Derek couldn't figure this guy out but proceeded to do his work with the Purchasing Department.

INTERNAL SALES AND SHIPPING DEPARTMENT: Internal Sales was run by a stressed out single mom named Kathy. You could tell at first glance that she had probably lived a rough life. Kathy was probably not college educated but had a lot of "street smarts." Kathy was cooperative with Derek. During the course of their interaction, Derek noticed how periodically there would be huge returns that were stacked nearly to the ceiling in the Shipping Department. When Derek inquired about these periodic huge returns, Kathy told him that sometimes they would ship orders to customers based on past purchasing habits even though the customer had not recently placed an order. As it turns out, when the customers saw a delivery at their door someone would just assume they had placed an order and would keep it. However, other customers would quickly return the supplies. "Was that a good business practice?" Derek inquired. "Well, we have to make our numbers at quarter's end—you have to do what you have to do," Kathy replied. On one of Derek's weekly flights home, he picked up a newspaper and began to read about all the current frauds. Man, it seems like every company is committing fraud these days, Derek thought to himself after seeing multiple fraud-related articles. Derek hadn't had any fraud training but began to wonder if his firm or the client he was working for could be committing fraud.

Questions

Based on the case data, comment on the following issues as they relate to possible fraud:

1. Derek's firm "selling" Derek to the client as an "SAP expert" though he hadn't even seen the software before
2. The unpredictable well-dressed purchasing manager.
3. The sales practices revealed in the Internal Sales Department.

INTERNET ASSIGNMENTS

1. Visit the Web site of the National White Collar Crime Center at www.nw3c.org. This site is funded through a grant from the Department of Justice. Its purpose is to assist federal law enforcement agencies in the investigation and prevention of white-collar crime. The center also has a college internship program. Click on the "Research" link, select "Papers, publications and reports," select "Papers," and then read the study on Embezzlement/Employee Theft from October 2009 and answer the following questions:

a. Research suggests that embezzlement accounts for approximately what percentage of all business failures[16]?
b. According to the study what percentage of employees steal from their employers?[17]

2. Go to www.fraud.org and learn about the National Fraud Information Center (NFIC). What does it do, and specifically, how does it make it easy for people to report fraud?

DEBATES

Fred is a friend of yours and works with you at the same company. He is a well-respected and trusted employee. He has two young children and is a leader in his community. You have discovered that Fred has embezzled $3,000 over a period of several years. While this is not much money for such a large company, you suspect that if you don't report him, the problem may get worse. On the other hand, he has young children, and he has done so much good in the company and the community. If you report him, he may go to prison because your company has an aggressive fraud prosecution policy. Should you report him or are there any other alternatives available?

END NOTES

1. Wells, J. T., 2007, *Corporate Fraud Handbook*, Hoboken, New Jersey: John Wiley & Sons, Inc.
2. Biegelman, M. T., Bartow, J. T., 2006, *Executive Roadmap to Fraud Prevention and Internal Control*, New Jersey: John Wiley & Sons, Inc.
3. Schwartz, M. S., Dunfee, T. W., and M. J. Kline, 2005, Tone at the Top: An Ethics Code for Directors, *Journal of Business Ethics*, Vol. 58: 1–3.
4. www.mental-health-matters.com/articles/article.php?artID=153, accessed May 22, 2004.
5. Wang, J.-M. and B. H. Kleiner, Effective Employment Screening Practices, *Management Research News*, Vol. 27: 4–5.
6. See, for example, W. Steve Albrecht, Conan C. Albrecht, and Ned C. Hill, "The Ethics Development Model Applied to Declining Ethics in Accounting," *Australian Accounting Review*, Issue 38, Vol. 16, No. 1 (March 2006): 30–40.
7. Trevino, L. K., Hartman, L. P. and M. Brown, 2000, Moral Person and Moral Manager: How Executives Develop a Reputation for Ethical Leadership, *California Management Review*, Vol. 42: 4.
8. For more information about situational honesty see Scott, E. D., 2000, Moral Values: Situationally Defined Individual Differences, *Business Ethics Quarterly*, Vol. 10: 2.
9. Stevens, B., 1999, Communicating Ethical Values: A Study of Employee Perceptions, *Journal of Business Ethics*, Vol. 20: 2.
10. Kaptein, M. and M. S. Schwartz, 2008, The Effectiveness of Business Codes: A Critical Examination of Existing Studies and the Development of an Integrated Research Model, *Journal of Business Ethics*, Vol. 77: 2.
11. Red Hat's Code of Business Conduct and Ethics can be found at http://investors.redhat.com/governance.cfm, accessed May 23, 2010.
12. Cottrell, D. M. and W. S. Albrecht, 1994, Recognizing the Symptoms of Employee Fraud, *Healthcare Financial Management*, Vol. 48: 5.
13. The names and setting in this case are fictitious.
14. Class-action lawsuits are permitted under federal and some state rules of court procedure in the United States. In a class-action suit, a relatively small number of aggrieved plaintiffs with small individual claims can bring suit for large damages in the name of an extended class. After a fraud, for example, 40 bondholders who lost $40,000 might decide to sue, and they can sue on behalf of the entire class of bondholders for all their alleged losses (say, $50 million). Lawyers are more than happy to take such suits on a contingency fee basis (a percentage of the judgment, if any).
15. http://money.cnn.com/galleries/2007/biz2/0705/gallery.contrarians.biz2/10.html
16. Bullard, P. and A. Resnick, 1983, SMR Forum: Too many hands in the corporate cookie jar, *Sloan Management Review*, Vol. 24: 3.
17. McGurn, J., 1988, Spotting the Thieves Who Work Among Us, *Wall Street Journal*, p. 16, March 7.

APPENDIX A

Red Hat Code of Business Conduct and Ethics

As Amended and Restated As of February 28, 2009

This Code of Business Conduct and Ethics (the "Code") sets forth legal and ethical standards of conduct for directors, officers and employees of Red Hat, Inc. and its subsidiaries (the "Company"). This Code is intended to deter wrongdoing and to promote the conduct of all Company business in accordance with high standards of integrity and in compliance with all applicable laws and regulations. This Code applies to the Company and all of its subsidiaries and other business entities controlled by it worldwide.

If you have any questions regarding this Code or its application to you in any situation, you should contact your supervisor or Red Hat's General Counsel.

Compliance with Laws, Rules and Regulations

The Company requires that all employees, officers and directors comply with all laws, rules and regulations applicable to the Company wherever it does business, including with respect to the conduct of business with governments and the protection of classified information. You are expected to be familiar with the laws, rules and regulations applicable to your place of work, and such additional laws, rules and regulations which may apply and of which the Company gives you written notice. With respect to conducting business with governments and associated governmental entities in the United States, please also consult Red Hat's Policy on Business Conduct for the United States Government Marketplace, which is available in the Legal section of the Company's Intranet.

You are expected to use good judgment and common sense in seeking to comply with all applicable laws, rules and regulations and to ask for advice when you are uncertain about them.

If you become aware of the violation of any law, rule or regulation by the Company, whether by its officers, employees or directors, it is your responsibility to promptly report the matter to your supervisor, the Red Hat General Counsel, or the Chairman of the Audit Committee of the Red Hat Board of Directors. While it is the Company's desire to address matters internally, nothing in this Code should discourage you from reporting any illegal activity, including any violation of the securities laws, antitrust laws, environmental laws or any other federal, state or foreign law, rule or regulation, to the appropriate regulatory authority. Employees, officers and directors shall not discharge, demote, suspend, threaten, harass or in any other manner discriminate against an employee because he or she in good faith reports any such violation. This Code should not be construed to prohibit you from testifying, participating or otherwise assisting in any state or federal administrative, judicial or legislative proceeding or investigation.

Conflicts of Interest

Employees, officers and directors must act in the best interests of the Company. You must refrain from engaging in any activity or having a personal interest that presents a "conflict of interest." A conflict of interest occurs when your personal interest interferes, or appears to interfere, with the interests of the Company. A conflict of interest can arise whenever you, as an officer, director or employee, take action or have an interest that prevents you from performing your Company duties and responsibilities honestly, objectively and effectively.

Employees and Officers. In the following instances a conflict of interest is deemed to exist absent mitigating facts and circumstances:

1. where the officer or employee performs services as a consultant, employee, officer, director, advisor or in any other capacity for, or has a financial interest in, a Direct Competitor of the Company, other than services performed in the context of the officer's or employee's job with the Company or at the request of the Company and other than a financial interest representing less than one percent (1%) of the outstanding shares of a publicly-held company;
2. where the officer or employee uses his or her position with the Company to influence a transaction with a Significant Supplier or Significant Customer in which such person has any personal interest, other than a financial interest representing less than one percent (1%) of the outstanding shares of a publiclyheld company;
3. where the officer or employee has any Close Relative who holds a financial interest in a Direct Competitor of the Company, other than an investment representing less than one percent (1%) of the outstanding shares of a publicly-held company;
4. where the officer or employee supervises, reviews or influences the performance evaluation or compensation of a member of his or her Immediate Family who is an employee of the Company; or
5. where the officer or employee engages in any other activity or has any other interest that the Board of Directors of the Company may reasonably determine to constitute a conflict of interest.

Directors. Directors must not:

1. perform services as a consultant, employee, officer, director, advisor or in any other capacity for, or have a financial interest in, a Direct Competitor of the Company, other than services performed at the request of the Company and other than a financial interest representing less than one percent (1%) of the outstanding shares of a publicly-held company;
2. have, or permit any Close Relative to have, a financial interest in a Direct Competitor of the Company, other than an investment representing less than one percent (1%) of the outstanding shares of a publicly-held company;
3. use his or her position with the Company to influence any decision of the Company relating to a contract or transaction with a Significant Supplier or Significant Customer of the Company if the director or a Close Relative of the director:
   - performs services as a consultant, employee, officer, director, advisor or in any other capacity for such Significant Supplier or Significant Customer; or
   - has a financial interest in such Significant Supplier or Significant Customer, other than an investment representing less than one percent (1%) of the outstanding shares of a publicly-held company.
4. directly supervise, review or influence the performance evaluation or compensation of a member of his or her Immediate Family; or
5. engage in any other activity or have any other interest that the Board of Directors of the Company may reasonably determine to constitute a conflict of interest.

For purposes of this Code, the following definitions apply:

"Close Relative" means a spouse, domestic partner, dependent child (including step-child) or any other person (other than a tenant or employee) sharing the person's household.

"Direct Competitor" means any commercial business entity which directly competes with one or more of the Company's product or service lines of business representing at least five percent (5%) of the Company's gross annual revenues.

"Immediate Family Member" of a person means that person's Close Relative and that person's child (including step-child), parent, stepparent, sibling, mother-in-law, father-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law and anyone else (other than a tenant or employee) sharing the person's household.

"Significant Customer" means a customer that has made during the Company's last full fiscal year, or proposes to make during the Company's current fiscal year, payments to the Company for property or services in excess of one percent (1%) of (i) the Company's consolidated gross revenues for its last full fiscal year or (ii) the customer's consolidated gross revenues for its last full fiscal year.

> "Significant Supplier" means a supplier to which the Company has made during the Company's last full fiscal year, or proposes to make during the Company's current fiscal year, payments for property or services in excess of one percent (1%) of (i) the Company's consolidated gross revenues for its last full fiscal year or (ii) the supplier's consolidated gross revenues for its last full fiscal year.

Participation in an open source project, whether maintained by the Company or by another commercial or non-commercial entity or organization does not constitute a conflict of interest even where such participant makes a determination in the interest of the project that is adverse to the Company's interests.

The rules set forth above are threshold rules. It is your responsibility to disclose to the General Counsel any transaction or relationship that reasonably could be expected to give rise to a conflict of interest, or, if you are an officer or director, to the Chairman of the Audit Committee of the Board of Directors (or in the case of such Chairman, to the Board of Directors), who shall be responsible for determining, based on all of the facts and circumstances, whether such transaction or relationship constitutes a conflict of interest. Determinations by the General Counsel of a conflict of interest may be appealed to the Audit Committee, and determinations by the Audit Committee of a conflict of interest, whether sustaining the General Counsel or made independently, may be appealed to the Board of Directors, which determination shall be final.

Upon a determination that a conflict exists, the finding party (General Counsel, Audit Committee or Board of Directors) must make an independent finding as to how the conflict of interest is to be mitigated. Mitigating actions include such measures as are reasonably certain to eliminate the conflict of interest, including, but not limited to reassignment of job duties, transfer of job assignment, termination of employment, or removal from office. All such mitigating actions are to be taken in accordance with the laws pertaining to the place of employment of the subject party, including laws governing due process and employment, and such other agreements of employment as may exist between the Company and the subject employee.

Insider Trading

Employees, officers and directors who have material non-public information about the Company or other companies, including our suppliers and customers, as a result of their relationship with the Company are prohibited by law and Company policy from trading in securities of the Company or such other companies, as well as from communicating such information to others who might trade on the basis of that information. To help ensure that you do not engage in prohibited insider trading and avoid even the appearance of an improper transaction, the Company has adopted an Insider Trading Policy, which is available in the Legal section of the Company's Intranet.

If you are uncertain about the constraints on your purchase or sale of any Company securities or the securities of any other company that you are familiar with by virtue of your relationship with the Company, you should consult with Red Hat's General Counsel before making any such purchase or sale.

Confidentiality

Employees, officers and directors must maintain the confidentiality of confidential information entrusted to them by the Company or other companies, including our suppliers and customers, except when disclosure is authorized by a supervisor or legally mandated. Unauthorized disclosure of any confidential information is prohibited. Additionally, employees should take appropriate precautions to ensure that confidential or sensitive business information, whether it is proprietary to the Company or another company, is not communicated within the Company except to employees who have a need to know such information to perform their responsibilities for the Company.

Third parties may ask you for information concerning the Company. Employees, officers and directors (other than the Company's authorized spokespersons) must not discuss internal Company matters with, or disseminate internal Company information to, anyone outside the Company, except as required in the performance of their Company duties and after an appropriate confidentiality agreement is in place. This prohibition applies particularly to inquiries concerning the Company from the media, market professionals (such as securities analysts, institutional investors, investment advisers, brokers and dealers) and security holders. All responses to inquiries on behalf of the Company must be made only by the Company's authorized spokespersons. If you receive any inquiries of this nature, you must decline to comment and refer the inquirer to your supervisor or one of the Company's

authorized spokespersons. The Company's policies with respect to public disclosure of internal matters are described more fully in the Noncompetition, Confidentiality and Assignment of Inventions Agreement which you signed at the time you joined the Company.

You also must abide by any lawful obligations that you have to your former employer. These obligations may include restrictions on the use and disclosure of confidential information, restrictions on the solicitation of former colleagues to work at the Company and non-competition obligations.

Finally, if you are involved in conducting business in the federal, state or local government marketplace(s), you may be subject to other obligations regarding the use, disclosure, safeguarding or receipt of particular types of information, including restrictions regarding competition-sensitive information such as government "source selection" or contractor bid and proposal information.

Honest and Ethical Conduct and Fair Dealing

Employees, officers and directors should endeavor to deal honestly, ethically and fairly with the Company's suppliers, customers, competitors and employees. Statements regarding the Company's products and services must not be untrue, misleading, deceptive or fraudulent. You must not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair-dealing practice.

Protection and Proper Use of Corporate Assets

Employees, officers and directors should seek to protect the Company's assets. Theft, carelessness and waste have a direct impact on the Company's financial performance. Employees, officers and directors must use the Company's assets and services solely for legitimate business purposes of the Company and not for any personal benefit or the personal benefit of anyone else.

Employees, officers and directors must advance the Company's legitimate interests when the opportunity to do so arises. You must not take advantage of opportunities for yourself or another person that are discovered through your position with the Company or the use of property or information of, or entrusted to, the Company.

Gifts and Gratuities

Employees, officers and directors must not accept, or permit any member of his or her Immediate Family to accept, any gifts, gratuities or other favors from any customer, supplier or other person doing or seeking to do business with the Company, other than items of nominal value. Any gifts that are not of nominal value should be returned immediately and reported to your supervisor. If immediate return is not practical, they should be given to the Company for charitable disposition or such other disposition as the Company believes appropriate in its sole discretion. For purposes of this policy, nominal value is considered $100 or less.

Common sense and moderation should prevail in the acceptance or provision of business entertainment for the Company. Employees, officers and directors should provide, or accept, business entertainment to or from anyone doing business with the Company only if the entertainment is infrequent, modest in light of the circumstances and intended to serve legitimate business goals.

It is not unusual for software and hardware companies in the Company's industry to offer free software and/or hardware to employees for testing purposes. If you are offered such equipment, you may accept it on behalf of the Company provided the equipment is necessary to your performance of your job or an open source project in which you participate and you notify the Company's General Counsel of the hardware or software contributed. All such donated hardware and software shall be the property of the Company.

Bribes and kickbacks are criminal acts, strictly prohibited by law. You must not offer, give, solicit or receive any form of bribe or kickback anywhere in the world.

You must also abide by the often stringent laws regulating gifts and gratuities to government officials and employees.

Accuracy of Books and Records and Public Reports

Employees, officers and directors must honestly and accurately report all business transactions. You are responsible for the material accuracy of your records and reports. Accurate record keeping and reporting are essential to the Company's ability to meet legal and regulatory obligations, including specific obligations relating to the Company's transactions with governments and governmental entities.

All Company books, records and accounts shall be maintained in accordance with all applicable regulations and standards and accurately reflect the true nature of the transactions they record in all material respects. The financial statements of the Company shall

conform in all material respects to generally accepted accounting rules and the Company's accounting policies. No undisclosed or unrecorded account or fund shall be established for any purpose. No false or misleading entries shall be made in the Company's books or records for any reason, and no disbursement of corporate funds or other corporate property shall be made without adequate supporting documentation.

It is the policy of the Company to provide full, fair, accurate, timely and understandable disclosure in reports and documents filed with, or submitted to, the Securities and Exchange Commission and in other public communications.

Concerns Regarding Accounting or Auditing Matters

Employees with concerns regarding questionable accounting or auditing matters or complaints regarding accounting, internal accounting controls or auditing matters may confidentially, and anonymously if they wish, submit such concerns or complaints in writing to the Chairman of the Audit Committee of the Board of Directors at the address listed below. See "Reporting and Compliance Procedures." A complete record of all complaints will be prepared by the Audit Committee each fiscal quarter and reported to the Board of Directors.

The Audit Committee will evaluate the merits of any concerns or complaints received by it and authorize such follow-up actions, if any, as it deems necessary or appropriate to address the substance of the concern or complaint.

The Company will not discipline, discriminate against or retaliate against any employee who reports a complaint or concern (unless the employee is found to have knowingly and willfully made a false report).

Waivers of this Code of Business Conduct and Ethics

While some of the policies contained in this Code must be strictly adhered to and no exceptions can be allowed, in other cases exceptions may be possible. Any employee or officer who believes that an exception to any of these policies is appropriate in his or her case should first contact his or her immediate supervisor. If the supervisor agrees that an exception is appropriate, the approval of the General Counsel must be obtained. The General Counsel shall be responsible for maintaining a complete record of all requests for exceptions to any of these policies and the disposition of such requests and report such record to the Audit Committee each fiscal quarter.

Any executive officer or director who seeks an exception to any of these policies should contact the Chairman of the Audit Committee of the Board of Directors. Any waiver of this Code for executive officers or directors or any change to this Code that applies to executive officers or directors may be made only by the Board of Directors of the Company and will be disclosed as required by law or stock market regulation.

Reporting and Compliance Procedures

Every employee, officer and director has the responsibility to ask questions, seek guidance, report suspected violations and express concerns regarding compliance with this Code. Any employee, officer or director who knows or believes that any other employee or representative of the Company has engaged or is engaging in Company-related conduct that violates applicable law or this Code should report such information to his or her supervisor, the Red Hat General Counsel, or to the Chairman of the Audit Committee of the Red Hat Board of Directors, as described below. You may report such conduct openly or anonymously without fear of retaliation. The Company will not discipline, discriminate against or retaliate against any employee who reports such conduct in good faith, whether or not such information is ultimately proven to be correct, or who cooperates in any investigation or inquiry regarding such conduct. Any supervisor who receives a report of a violation of this Code must immediately inform the General Counsel.

You may report violations of this Code on a confidential or anonymous basis by calling Red Hat's Corporate Governance Hotline. Depending on the nature of the information you are providing, your message will be directed to either the Chairman of the Audit Committee or the General Counsel. Instructions are provided on the Hotline. While we prefer that you identify yourself when reporting violations so we may follow up with you as necessary for additional information, you may leave messages anonymously if you wish.

If either the General Counsel or the Chairman of the Audit Committee receives information regarding an alleged violation of this Code, he or she shall, as appropriate, (a) evaluate such information, (b) if the alleged violation involves an executive officer or a director, inform the Chief Executive Officer and Board of Directors of the alleged violation, (c) determine whether it is necessary to conduct an informal inquiry or a formal investigation and, if so, initiate such inquiry or

investigation and (d) report the results of any such inquiry or investigation, together with a recommendation as to disposition of the matter, to the Board of Directors or a committee thereof. Employees, officers and directors are expected to cooperate fully with any inquiry or investigation by the Company regarding an alleged violation of this Code. Failure to cooperate with any such inquiry or investigation may result in disciplinary action, up to and including discharge.

The Company shall determine whether violations of this Code have occurred and, if so, shall determine the disciplinary measures to be taken against any employee who has violated this Code. In the event that the alleged violation involves an executive officer or a director, the Chief Executive Officer and the Board of Directors, respectively, shall determine whether a violation of this Code has occurred and, if so, shall determine the disciplinary measures to be taken against such executive officer or director.

Failure to comply with the standards outlined in this Code will result in disciplinary action including, but not limited to, reprimands, warnings, probation or suspension without pay, demotions, reductions in salary, discharge and restitution. Certain violations of this Code may require the Company to refer the matter to the appropriate governmental or regulating authorities for investigation or prosecution. Moreover, any supervisor who directs or approves of any conduct in violation of this Code, or who has knowledge of such conduct and does not immediately report it, also will be subject to disciplinary action, up to and including discharge. All such disciplinary actions are to be taken in accordance with the laws pertaining to the place of employment of the subject party, including laws governing due process and employment, and such other agreements of employment as may exist between the Company and the subject employee.

Dissemination and Amendment

This Code shall be distributed annually to each employee, officer and director of the Company, and each employee, officer and director shall certify that he or she has received, read and understood the Code and has complied with its terms.

The Company reserves the right to amend, alter or terminate this Code at any time for any reason. The most current version of this Code can be found in the Legal section of the Company's Intranet.

This document is not an employment contract between the Company and any of its employees, officers or directors and does not alter any existing employment contract, if any, or, where no such employment contracts exists, the Company's at-will employment policy.

Certification

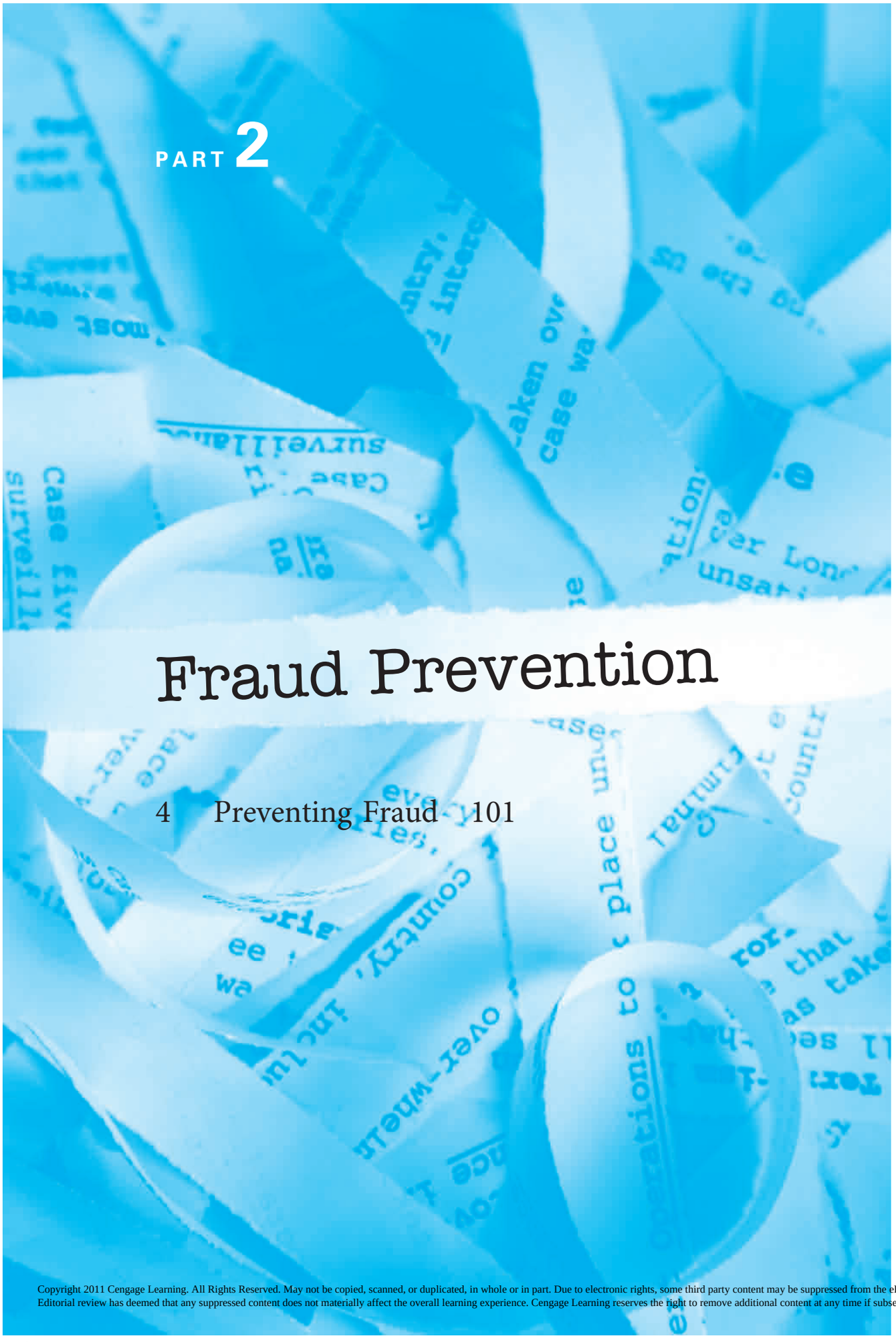
I, _____ do hereby certify that:
(Print Name Above)

1. I have received and carefully read the Code of Business Conduct and Ethics of Red Hat, Inc., as amended and restated on February 28, 2009, and the Red Hat Insider Trading Policy.
2. I understand the Code of Business Conduct and Ethics and the Red Hat Insider Trading Policy.
3. I will comply with the terms of the Code of Business Conduct and Ethics and the Red Hat Insider Trading Policy.

Date: _____

(Signature)

EACH EMPLOYEE, OFFICER AND DIRECTOR IS REQUIRED TO RETURN THIS CERTIFICATION TO THE HUMAN CAPITAL DEPARTMENT WITHIN 14 DAYS OF REQUEST. FAILURE TO DO SO MAY RESULT IN DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION.



PART 2

Fraud Prevention

This page was intentionally left blank

CHAPTER 4

Preventing Fraud

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- **Understand how to create a culture of honesty, openness, and assistance.**
- **Know how to eliminate opportunities for fraud.**
- **Understand how to create an effective organization to minimize fraud.**
- **Understand the importance of proactive fraud auditing.**
- **Understand the importance of creating a comprehensive approach to fighting fraud.**

TO THE STUDENT

The past three chapters were introductory. Chapter 4 is the first chapter that deals with fighting fraud, in this case, preventing fraud. The chapter identifies two major ways that organizations can work to prevent fraud: (1) create a culture of honesty, openness, and assistance; and (2) eliminate opportunities for fraud. There are several ways to do each of these which are covered in the chapter. You should realize, however, that no matter how good an organization's fraud prevention efforts are, an organization will never prevent all fraud using cost-effective techniques.

Margaret worked for First National Bank. For 34 years, she was an honest and trusted employee. In the three years prior to her retirement, she embezzled over $600,000. The fraud was discovered after she retired. Once the fraud was known, Margaret and the bank suffered tremendous adverse consequences. The bank lost several customers and was the subject of numerous negative articles about the fraud. The bank also spent significant amounts of time investigating the fraud and dealing with the negative effect on other employees. As for Margaret, the bank took possession of her home and her retirement account. Her husband, who supposedly had no knowledge of the fraud, voluntarily contributed the proceeds of his retirement account from another company to the bank. The bank took possession of virtually every asset the couple owned. In addition, Margaret still owes the bank over $200,000 and has entered into a restitution agreement to make regular payments toward meeting the agreement. Margaret was prosecuted and incarcerated for one year. All of her friends and family members, including her children and grandchildren, know that she is a convicted felon. When Margaret was released from prison, she was ordered by the judge to seek active employment so she could start making restitution payments. If she fails to make regular payments, she violates her parole agreement and must return to jail. Margaret and her husband suffered tremendous embarrassment from the fraud. When Margaret's fraud was written up in local newspapers, many of her long-time friends called her and the bank to learn more about the fraud. The bank was required to submit a criminal referral form to the Office of the Controller of the Currency (OCC). By law, the OCC was required to submit a copy of the referral form to the FBI and the IRS. The FBI investigated Margaret, and the IRS came after her. The IRS levied fines, penalties, interest, and back taxes on Margaret because she had over $600,000 in income that she had failed to report on her tax returns. (Although in subsequent negotiations, the portion she paid back by giving the bank her assets was determined to be a nontaxable loan.) Margaret will probably always have difficulty getting a job, buying life or car insurance, or doing many other things without informing people that she is a convicted felon. In many ways, Margaret's life and reputation have been ruined.

As you can see from this example, there are no winners when fraud occurs. The results are the same in management fraud cases as well. Take the case of Adelphia, for example, where John Rigas and his son, Timothy, were convicted of orchestrating a massive management fraud on investors in Adelphia Communications Corp. As for the perpetrators, John Rigas, the 80-year-old founder of the cable company, was given a 15-year prison sentence. The judge who passed sentence said that he would have jailed Rigas for much longer if not for his age and poor health. John's son, Timothy, who was the company's former chief financial officer, was sentenced to 20 years. The perpetrators weren't the only losers. Adelphia declared bankruptcy following the frauds costing shareholders of the company approximately $25 billion, making it one of the largest bankruptcies in U.S. history. Hundreds of fraud investigators, lawyers, accountants, and others spent years trying to determine exactly what happened. Civil cases surrounding the fraud—against banks, accountants, and others related to their work with Adelphia—will continue for years.

At best, a person who commits fraud may enjoy a higher lifestyle or keep a company from failing for a while.[1] Organizations or individuals from whom funds

are stolen are also losers. In Margaret's case, the bank's name was splashed across the front pages of the local newspapers. Some customers terminated business relationships with the bank for fear that "if the bank can't safeguard funds, then my money is not safe there." The bank also lost the money that Margaret hasn't yet paid (over $200,000), plus interest on the $600,000 that she embezzled. Margaret will probably never be able to pay back the entire sum she stole, because the kinds of jobs that were available to her upon release from prison don't pay much. In addition, bank employees spent hundreds of hours investigating, preparing legal defenses, and testifying in the case. In the end, dishonesty cost both the victims and the perpetrators much more than they embezzled.

Clearly, fraud prevention is where the big savings occur. When fraud is prevented, there are no detection or investigation costs. There are no bad apples—no examples of fraud in the organization. The organization doesn't have to make tough termination and prosecution decisions. Valuable work time is not lost to unproductive activities and dealing with crises.

Just About Everyone Can Be Dishonest

It would be nice to believe that most individuals and most employees are so honest that they would never commit fraud and, therefore, the kind of culture an organization creates and the fraud opportunities that exist aren't important. Unfortunately, that is not the case. Most people are capable of committing fraud, and most people adapt to their environments. When placed in an environment of low integrity, poor controls, loose accountability, or high pressure, people tend to become increasingly dishonest. There are numerous examples of companies where top management's dishonest practices were adopted by workers after seeing the bad modeling by top executives. In the famous Equity Funding case, for example, management created fictitious policyholders and wrote insurance policies on them. The fraudulent policies were then sold to other insurance companies or reinsurers. An employee of the company, who observed the dishonest behavior, thought to himself, "I might as well get in on the action. It doesn't make sense that all these fake insurance policies are written and no one ever dies." Therefore, he started causing a few of the fictitious people to "die" and personally collected the death proceeds.

STOP & THINK *Do you agree with the statement that most people are capable of committing fraud? Do you believe that you could ever commit fraud?*

Organizations can create either a low-fraud or a high-fraud environment. In this chapter, we identify two essential factors involved in a low-fraud environment that are important in preventing fraud. The first involves creating a culture of honesty, openness, and assistance—attributes of a low-fraud environment. The second involves eliminating opportunities to commit fraud and creating expectations that fraud will be punished. At the end of the chapter, we show how fraud prevention, detection, and investigation efforts should be combined to provide a comprehensive fraud-fighting program for a company.

Creating a Culture of Honesty, Openness, and Assistance

Three major factors in fraud prevention relate to creating a culture of honesty, openness, and assistance. These three factors are (1) hiring honest people and providing fraud awareness training; (2) creating a positive work environment, which means having a well-defined code of conduct, having an open-door policy, not operating on a crisis basis, and having a low-fraud atmosphere; and (3) providing an employee assistance program (EAP) that helps employees deal with personal pressures.

Hiring Honest People and Providing Fraud Awareness Training

Effectively screening applicants so that only "honest" employees are hired is very important. As stated earlier in this book, studies have indicated that nearly 30 percent of Americans are dishonest, 40 percent are situationally honest, and only about 30 percent are honest all the time. Nonpublic studies conducted at firms with which we have consulted have also shown that 25 percent of all frauds are committed by employees who have worked three years or less. Individuals with gambling, financial, drug, or past criminal problems should not be hired, or, at least, if they are hired, the adverse information about their backgrounds or characters should be known.

As an example of how prevalent lying is by potential recruits, consider the following excerpts from an online article about lying on résumés by Andrea Kay.[2]

> *Lying on résumés is apparently on the rise, according to several surveys. A Knight-Ridder-Tribune Business News article reported that an online survey conducted by the Society for Human Resource Management determined that more than 60 percent of the 373 human resource professionals who responded found inaccuracies on résumés. Nearly half the respondents to a Korn/Ferry online survey said 44.7 percent of their 300 respondents said they believed résumé fraud among executives is increasing.*
>
> *What do they lie about? "About 71 percent of the résumés misrepresent the number of years they've worked on a job," said Jeff Christian, chairman of the search firm Christian & Timbers in an interview on NPR's program, Talk of the Nation.*
>
> *"Next, they exaggerate accomplishments such as taking credit for something they didn't do or misrepresent the size of an organization they managed," he said. Most often people fabricate reasons for leaving a previous job, according to the Korn/Ferry survey.*
>
> *In 2003, an employee screening firm in London reported that its research suggests lying on résumés is growing around the world, with the number of people who falsify information jumping 15 percent between 2001 and 2002, according to the Institute of Management & Administration.*

With today's stringent privacy laws, it is essential that companies have good employee screening policies. Even in a highly controlled environment, dishonest employees with severe pressures often commit fraud. Résumé verification and certification are two tactics that organizations should use to prevent fraud. One of the most important responsibilities of an employer is the hiring and retention of its employees. In today's market, turnover tends to be high and employee loyalty may be low.

Poor hiring decisions may not only lead to hiring employees who are dishonest but also under a negligent hiring and/or retention claim, an employer may be liable for acts or omissions of the employee, either within or outside the scope of the employee's employment, as long as the injured party can show specific negligent acts of the employer itself. An example of negligent hiring and/or retention claims includes a trucking company liable for a wrongful death resulting from one of its truckers driving drunk on the wrong side of the road and colliding with an oncoming car, killing the driver. The trucking company failed to verify the trucker's claimed perfect driving record, which would have shown numerous prior DUI violations.

Another example is a church member who was raped during counseling sessions with a church employee. In his lawsuit, the church member claims that the church should not have had the church employee in a counseling position, especially in light of his prior record of sexual offenses during such sessions.

No employer can totally immunize itself from hiring fraudulent employees or from liability for claims asserting negligent hiring and/or negligent retention. However, the employer that follows the following recommendations as part of its hiring and retention policies and practices will be as successful as possible in avoiding frauds and negligent hiring claims.

First, before hiring an applicant for any position, especially key management positions, the employer should verify all information on the applicant's résumé and/or application. The verification should be complete and conducted by an employee who is thorough and persistent in this important procedure. There is no question that verifying an applicant's résumé and/or application is a resource-consuming process. (In the case of a top executive, you should make sure that a search firm that is hired verifies all information on candidates' résumés.) The benefits of such precautions include increased knowledge of the applicant and his or her propensity to be truthful as well as significant reduction in hiring and retaining dangerous, unfit, or dishonest employees. As an example of a CEO who lied on his résumé, consider the case of RadioShack's CEO David Edmondson.[3] Edmondson resigned after the *Star-Telegram* of Fort Worth, Texas, reported he had lied on his résumé.

Edmondson claimed degrees in both theology and psychology from Pacific Coast Baptist College in California. The school's registrar told the *Star-Telegram* that records showed Edmondson had completed two semesters and that the school had never offered degrees in psychology.

Other prominent people who have recently lied on their résumés include the mayor of Rancho Mirage, California, who admitted he didn't hold degrees that he'd claimed, a former football coach at Notre Dame,

and a former spokesman for NASA. A recent congressional investigation uncovered 463 federal employees who had credentials from unaccredited schools giving bogus degrees. A recent example of resume embellishment is Gregory Probert, COO of Herbalife who stated that he obtained an M.B.A. from UCLA. After a report by the Fraud Discovery Institute, Probert admitted that he faked his degree and resigned in May, 2008.

An important part of the employer's verification of all information on the applicant's résumé and/or application is verification of the applicant's references. Due to statutory restrictions on the dissemination of such information and the applicant's reasonable expectation of privacy, employers should always obtain a written authorization and/or a "hold harmless agreement" from the applicant to obtain information from references.

CAUTION *When conducting job-seeking interviews, the interviewer must be very careful not to ask discriminatory questions, or base an evaluation of the applicant on criteria that are of a discriminatory nature. Many discrimination complaints and lawsuits are filed against employers from job-seeking interviews. Many government and state laws must be followed when conducting interviews, including the Federal Equal Employment Opportunity Commission (EEOC) which enforces EEO laws such as Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act (ADEA), and the Americans with Disabilities Act (ADA). Most states have their own Human Rights Acts as well that must be complied with. Questions that deal with an applicant's race, sex, age, religion, color, national origin, or disability are usually prohibited unless the criterion is a bona fide occupational qualification. Whether asked on an application form or in an interview, the federal and state agencies mentioned above will consider questions on the subjects listed below as evidence of discrimination, unless the employer is able to show that the inquiries are job-related or that there is a business necessity for asking the question.*

1. *Arrest records*
2. *Garnishment records*
3. *Marital status*
4. *Child-care provisions*
5. *Contraceptive practices—questions such as "What kind of birth control method do you use?"*
6. *Pregnancy and future childbearing plans*
7. *Physical or mental disabilities*
8. *Height and weight*
9. *Nationality, race, or ancestry*

Second, the employer should require all applicants to certify that all information on their application and/or résumé is accurate. A requirement that all applicants must affirm the truth of the matters set forth in their application and/or résumé will act as a deterrent against false or misleading statements or omissions. The application should provide, in writing acknowledged and agreed to by the applicant, that, in the event false information in the form of statement or omission is discovered on the application and/or résumé, then such discovery is grounds for immediate termination.

Third, the employer should train those involved in the hiring process to conduct thorough and skillful interviews. Interviewing prospective employees is one of the most important activities employers do. The employer's objective of an interview is to determine whether an applicant is suitable for an available position. The interview provides the employer an opportunity to obtain in-depth information about a job applicant's skills, work history, and employment background.

Many prudent employers require interviewers to ask a standard set of questions designed to obtain certain information from the application. The interviewer is then left to her own discretion to follow up and/or ask additional questions during the course of the interview. Numerous companies specialize in helping companies hire the right employees, ask the right hiring questions, and avoid legal traps by asking illegal questions.

There are also other ways to be creative in hiring processes. Many financial institutions, for example, now use systems to determine whether prospective employees and customers have had past credit problems. Banks are also fingerprinting new employees and customers and comparing the fingerprints with law enforcement records. Other organizations are hiring private investigators or using publicly available databases to search information about people's backgrounds. Some organizations are administering drug tests. Pen-and-pencil honesty tests are also being used as a screening tool.

One company, for example, extensively trained several interviewers to know which questions were legal to ask and which were illegal, to recognize deception and lying, and to probe legally into applicants' backgrounds. It also adopted a policy of calling three previous references instead of one. It developed a rule that if no gratuitously positive information was received in any of the three background checks, these checks would be viewed as negative. (The interviewers tried to call references who personally knew the applicants, rather than personnel officers who didn't know them.) Over a three-year period, this company found that 851 prospective employees, or

14 percent of all applicants, had undisclosed problems, such as previous unsatisfactory employment, false education or military information, criminal records, poor credit ratings, alcoholism, or uncontrolled tempers. People with these types of problems generally find it easier to rationalize dishonest acts, and preventing such people from being hired can reduce fraud.

Remember this …

Verify all information on the applicant's résumé and/or application using the following suggestions:

1. *Require all applicants to certify that all information on their application and/or résumé is accurate.*
2. *Train those involved in the hiring process to conduct thorough and skillful interviews.*
3. *Use industry-specific or other approaches as deemed necessary (credit checks, fingerprinting, drug tests, public record searches, honesty tests, etc.).*

As an example of poor screening, consider the following actual fraud:

A controller defrauded his company of several million dollars. When the fraud was investigated, it was discovered that he had been fired from three of his previous five jobs, all in the last eight years. He was discovered when the CEO came to the office one night and found a stranger working in the accounting area. The nocturnal stranger was a phantom controller who was actually doing the work of the hired "corporate controller," who wasn't even trained in accounting.

Once people have been hired, it is important to have them participate in an employee awareness program that educates them about what is acceptable and unacceptable, how all parties, including them, are hurt when someone is dishonest, and what actions they should take if they see someone doing something improper. A comprehensive awareness program should educate employees about how costly fraud and other types of business abuses are. Employees must know that fraud takes a bite out of their pay and benefits, as well as corporate profits and returns to shareholders, and that no dishonest acts of any kind will be tolerated. Most companies with successful fraud awareness programs have packaged fraud training with other sensitive issues important to employees, such as employee safety, discrimination, substance abuse, and the availability of EAPs.

One company, for example, educates all employees about abuses and gives them small cards to carry in their purses or wallets. The cards list four possible actions employees can take if they suspect abuses are taking place. They can (1) talk to their immediate supervisor or management, (2) call corporate security, (3) call internal audit, or (4) call an 800 hotline number. Employees are told that they can either provide hotline information anonymously or disclose their identities. This company has also made several videos about company abuses, including frauds, which are shown to all new employees. New posters relating to the awareness program are posted conspicuously throughout the organization on a regular basis. Because of these awareness programs, fraud and other abuses have decreased substantially.

Creating a Positive Work Environment

The second factor important in a culture of honesty, openness, and assistance is creating a positive work environment. Positive work environments do not happen automatically; rather, they must be cultivated. It is a fact that employee fraud and other dishonest acts are more prevalent in some organizations than in others.

Organizations that are highly vulnerable to fraud can be distinguished from those that are less vulnerable by comparing their corporate climates. Three elements that contribute to the creation of a positive work environment, thus making the organization less vulnerable to fraud, are (1) creating expectations about honesty through having a good corporate code of conduct and conveying those expectations throughout the organization, (2) having open-door or easy access policies, and (3) having positive personnel and operating procedures.

Setting proper expectations is a powerful tool in motivating employees to behave honestly. Consider the following story about expectations:

Imagine Miss Periwinkle, a fourth-grade teacher, arriving for class on the first day of school. Before she enters her classroom, the principal stops her in the hall.

"Miss Periwinkle, there's something you should know about this class. We've placed all the bright and talented children on the right side of the room. On the left, we've seated the ones we know are slower and lack motivation. We thought the seating arrangement would help you in your teaching."

Armed with this information, she begins a semester of instruction. But there's a catch. There are no divisions of intelligence or motivation in this classroom; those on both sides of the room were randomly

selected from a group of equally able and motivated students. They are part of an experiment to determine if the teacher's expectations will affect the children's learning and testing.

This is a hypothetical recasting of various psychological experiments done many times over the last 30 years. The results are invariably the same. Students the teacher thinks are "smart" score well on tests; the "dull" ones don't do as well. The difference is not a result of biased grading; the "dull" ones really have learned less. Why?

The explanation is often described as the Pygmalion effect. Sterling Livingston, writing in the *Harvard Business Review* (September 1988), extended this phenomenon into management with a simple thesis: People generally perform according to a leader's expectations. If expectations are low, actual performance is likely to be "substandard." If, however, expectations are high, performance is usually high as well. "It is as though there were a law that caused subordinates' performance to rise or fall to meet management's expectations," Livingston wrote.

Livingston and others have also found that expectations must be genuine and accepted by leaders. The studies have concluded that people know when they are being conned. If expectations are unrealistically high or if they are not being taken seriously by leaders, people know it. Conversely, if a manager pretends that he has confidence and high expectations when he really has doubts, people will know that, too.

The lesson about expectations is clear: People have keen senses about expectations. You can't fool them; expectations must be genuine. Trying to create expectations, especially about integrity and ethics, when top management isn't serious about the expectations, only erodes their credibility.

According to the researchers, a good axiom to remember is, "What you expect is what you'll get."[4] As an example of the power of expectations, consider the following true story.

A wife told her husband that she had accepted an invitation for the two of them to be chaperons at a high school dance where their daughter attended. The husband wasn't excited about the assignment but agreed to go. At the dance, his wife seemed very unhappy and at one point ran out of the building crying. Following her out, the husband asked, "Why are you so unhappy? I came to this dance with you even though I really didn't want to. I thought I was being a good husband." Still crying, she said "Can't you see it? Every other husband who is here as a chaperon bought his wife a corsage but you didn't." The wife's expectation was not only that the husband would attend the dance but that he would also get her a corsage like other chaperoning husbands.

One way to create and communicate clear expectations about what is and is not acceptable in an organization is to have an articulated code of conduct. Section 406 of the Sarbanes-Oxley Act of 2002, "Code of Ethics for Senior Financial Officers," requires that every public company have a code of ethics for management and its board of directors. Shortly after Congress passed the Sarbanes-Oxley Act, the Securities and Exchange Commission (SEC) revised its listing standards to require public companies to create and distribute a code of conduct to all employees. Merely having a code of conduct, however, is not sufficient. It must be visible and communicated frequently. Some companies have found it helpful to even have employees read and sign their code annually and certify that they have not violated the code or seen others who have. In Chapter 3, we included the code of conduct for Red Hat, Inc. As another example of a good code of ethics for all employees, consider the code of Hormel Foods shown in Figure 4.1.

Hormel's code not only clarifies what is and is not acceptable, but it also specifies the disciplinary action that will be applied to violators and provides contact (whistle-blower) information for reporting violations. If Hormel is successful in keeping this code in front of its employees, just the mere fact that everyone knows that others know what is expected, what expected punishments are, and how to escalate information about violations should reduce the number of dishonest incidents in the company.

Literature on moral development suggests that if you want someone to behave honestly, you must both label and model honest behavior. As we have discussed, a clearly defined code of conduct labels for employees what is acceptable and unacceptable. Having employees periodically read and sign a company code of ethics reinforces their understanding of what constitutes appropriate and inappropriate behavior. A clearly specified code inhibits rationalizations, such as "It's really not that serious," "You would understand if you knew how badly I needed it," "I'm really not hurting anyone," "Everyone is a little dishonest," or "I'm only temporarily borrowing it." When a company specifies what is acceptable and what is unacceptable and requires employees to acknowledge that they understand the

FIGURE 4.1 HORMEL FOODS CODE OF CONDUCT

Code of Ethical Business Conduct

Introduction

This Code of Ethical Business Conduct ("Code") covers a wide range of business practices and procedures. It does not cover every issue that may arise, but it sets out basic principles to guide all employees, officers and directors of the Company. Obeying the law, both in letter and in spirit, is the foundation on which this Company's ethical standards are built. All of the Company's employees and directors must conduct themselves accordingly and seek to avoid even the appearance of improper behavior. All employees, officers and directors must respect and obey the laws of the cities, states and countries in which they operate.

Conflict of Interest

A "conflict of interest" exists when a person's private interests interfere in any way with the interests of the Company. All employees, officers and directors should avoid any personal activity or participation in any venture which may create a conflict with their responsibility to protect and promote the best interests of the Company. Employees, officers and directors should assure that their spouses and dependents avoid any activity which would constitute a conflict of interest if engaged in by the employee, officer or director. For example, any activity which would allow you, or a member of your immediate family, to enjoy personal gain or benefit as a result of your employment relationship with the Company would be considered a conflict of interest.

Gifts

No gift, loan or favor should be made to or accepted by employees, officers, directors or their immediate families involving any supplier, customer, or others with whom the Company does business if it is intended to influence a business decision. This does not prohibit casual entertainment, business entertainment consistent with the Company's usual practices, or gifts which are reasonably viewed under the circumstances in which they are given or received to be of nominal value. For this purpose, any gift in kind of less than $100 would be considered of nominal value. Acceptance of cash or cash equivalents is not acceptable under any circumstances. By way of example, attendance at a professional sporting event as a guest of a supplier or customer would constitute business entertainment consistent with the Company's usual practices; however, the receipt of tickets to the same event from a supplier or customer without the attendance of the supplier or customer would be viewed as a gift which must be of nominal value.

Corporate Opportunities

Employees, officers and directors are prohibited from taking for themselves personally opportunities that are discovered through the use of corporate property, information or position without the consent of the Board of Directors. No employee, officer or director may use corporate property, information, or position for improper personal gain, and no employee may compete with the Company directly or indirectly. Employees, officers and directors owe a duty to the Company to advance the Company's legitimate interests when the opportunity to do so arises.

Illegal Payments

Any payments by the Company to the United States or foreign persons or companies are prohibited if the payments would be illegal under the Foreign Corrupt Practices Act of 1977 or other United States or foreign laws. This prohibition includes any payments to government officials or their agents, domestic or foreign, unless Company counsel has advised the payment is legal and acceptable. It is never acceptable to pay any third party anywhere an undisclosed commission, kickback or bribe to obtain business.

Illegal Political Contributions

Corporate funds and other assets shall not be used for any illegal political contribution. This prohibition includes any political contribution unless otherwise advised by Company counsel. Employees are encouraged to make personal contributions to candidates and political parties of their choice.

Protection and Proper Use of Company Assets

All employees, officers and directors should endeavor to protect the Company's assets and ensure their efficient use. The use of any funds or other assets of, or the providing of any services by, the Company for any purpose which is unlawful under applicable laws of the United States, any state thereof, or any foreign jurisdiction, is prohibited. Employees, officers and directors may not use employees, materials, equipment or other assets of the Company for any unauthorized purpose.

(continued)

FIGURE 4.1 CONTINUED

Proper Accounting

Employees, officers and directors must comply with prescribed accounting, internal accounting, and auditing procedures and controls at all times. All records must accurately reflect and properly describe the transactions they record. All assets, liabilities, revenues and expenses shall be properly recorded on a timely basis in the books of the Company.

Insider Trading

Employees, officers and directors shall not buy or sell Company stock or make recommendations regarding it based upon insider information. Insider information is material information that is not generally known by those outside the Company that could affect the value of the Company's stock.

Confidential Information

Employees, officers and directors may not directly or indirectly use or disclose any secret or confidential knowledge or data of the Company, except as authorized in their ordinary course of employment or as required by law. Any notes, memoranda, notebooks, drawings or other documents made, compiled or delivered to employees during the period of their employment are the exclusive property of the Company and must be turned over to it at the time of termination of their employment or at any other time upon the Company's request. Additionally, while it is appropriate to gather information about the Company's markets, including publicly available information regarding competitors, employees and officers should not seek to acquire proprietary and confidential information of competitors by unlawful or unethical means, including information resulting in the breach of nondisclosure obligations by competitors' employees or other third parties.

Inventions, Developments, Improvements

Any inventions, developments or improvements which are conceived by employees during their period of employment by the Company must be promptly disclosed to the Company in writing, and will in most cases be the Company's exclusive property. Inventions which were developed on an employee's own time and are not related to the Company's business or research would not be the Company's property.

Antitrust Compliance

Activity which violates the antitrust laws of the United States, any state thereof, or comparable laws of foreign jurisdictions, is prohibited. Employees, officers and directors must comply with all antitrust compliance policies adopted by the Company. Areas in which employees, officers and directors must be sensitive to antitrust problems include pricing, termination of existing relationships with customers or suppliers, the establishment of either exclusive customers or suppliers, tie-in sales, boycotts and reciprocity.

Fair Dealing

Employees, officers and directors must observe the highest ethical standards in relationships with competitors, suppliers and customers. Each employee, officer and director should endeavor to respect the rights of, and deal fairly with, the Company's customers, suppliers, competitors and employees. No employee, officer or director should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other intentional unfair-dealing practice.

Harassment

All employees have a right to work in an environment free of harassment, and the Company prohibits harassment of its employees in any form—by supervisors, co-workers, customers, or suppliers.

Safety

All employees have a right to work in a safe environment, and all safety rules as well as common safety practices must be followed. Conduct which is unsafe, including possession or being under the influence of a controlled substance on Company premises or Company time, is prohibited.

Government Reporting

Employees, officers and directors must assure that any reports to any listing agency, or any governmental unit or agency in the United States or abroad, including the Securities and Exchange Commission, and the Internal Revenue Service, made by them or under their supervision, are honest, accurate and complete.

The Chief Executive Officer and the Chief Financial Officer of the Company are responsible for full, fair, accurate, timely and understandable disclosure in the periodic reports required to be filed by the Company

(continued)

FIGURE 4.1 CONTINUED

with the Securities and Exchange Commission. As a result, the Chief Executive Officer and Chief Financial Officer of the Company shall promptly bring to the attention of the Director of Internal Audit any material information of which they become aware that could affect the disclosures made by the Company in its public filings.

Environmental Responsibility

All employees, officers and directors are required to comply with all applicable federal, state and local laws and regulations relating to the protection of the environment, as well as any requirements which pertain to the Company's operations outside the United States. Additionally, employees, officers and directors must comply with all environmental policies adopted by the Company.

Product Integrity

The Company's products and their labeling must reflect the integrity of the Company and its employees. All Company products must be produced, labeled and handled in keeping with the Company's high standards of sanitation, and in compliance with all Company specifications and governmental requirements for content and process, to produce safe and wholesome, high quality and accurately labeled products.

Diversity

The Company welcomes diversity in its employees, suppliers, customers, and others with whom the Company does business. The Company is affirmatively committed to providing the same opportunities for success to all individuals, regardless of race, religion, national origin, age, sex, or disability. All employees are expected to share in and support that commitment.

Fair Employment Practices

In addition to prohibiting harassment and providing a safe workplace, the Company and its employees, officers and directors must comply with all applicable laws governing employment. Discrimination on account of race, religion, national origin, sex, age, disability, or status as a veteran will not be tolerated.

Foreign Trade

Employees involved in foreign trade operations are expected to maintain an awareness of, and comply with, the requirements of the U.S. Antiboycott Laws, the U.S. Trade Embargo Regulations, and any other U.S. or foreign laws applicable to the Company's foreign trading operations. The U.S. Antiboycott Laws prohibit U.S. companies and their foreign subsidiaries from entering into agreements in support of any foreign boycott which has not been sanctioned by the U.S. government. The U.S. Trade Embargo Regulations prohibit U.S. companies and their foreign subsidiaries from entering into transactions with countries with whom the U.S. government maintains a trade embargo, as well as with entities that are owned or controlled by those countries.

Responsible Delegation

Discretionary authority must not be delegated to anyone, within or on behalf of the Company, where there is reason to believe that individual might engage in illegal activities.

Disciplinary Action

While the Company relies on the voluntary compliance with this Code by each employee, officer and director as a matter of personal integrity, disciplinary action will be taken in appropriate instances. Such instances include: actions which violate this Code; withholding information regarding violations; supervision which is inadequate to the point of evidencing a negligent or willful disregard for this Code in connection with a violation; and any form of retaliation against an employee reporting a violation. Disciplinary action may include suspension, termination, recovery of damages, or criminal prosecution.

Reporting Illegal, Unethical Behavior, or Violations of the Code

With the exception of concerns or complaints regarding questionable accounting or auditing matters, or internal accounting controls which must be promptly forwarded directly to the Audit Committee of the Board of Directors, any employee, officer or director who observes or otherwise becomes aware of any illegal, unethical behavior, or any violation of the Code shall report the violation to a supervisor, the General Counsel, or the Director of Internal Audit, or he or she may report the matter to any member of the Audit Committee of the Board of Directors. Additionally, employees, officers and directors may report any violation, or suspected violation, of the Code, including concerns regarding questionable accounting or auditing matters, by using the anonymous "Hot Line"

(continued)

FIGURE 4.1 CONTINUED

established for this purpose. The telephone number for this Hot Line is: 1-800-750-4972.

Employees and officers are encouraged to talk to supervisors, managers or other appropriate personnel when in doubt about the best course of action to take in a particular situation. It is the policy of the Company not to allow retaliation for reports of misconduct by others made in good faith by employees. Employees are expected to cooperate in internal investigations of misconduct.

Waivers of the Code

Every effort will be made to resolve potential conflicts of interest or other ethics code situations when these are disclosed promptly to management, and the parties involved have acted in good faith. In the unlikely event that potential conflicts cannot be resolved, waivers will only be given for matters where appropriate. Any waivers for executive officers and directors must be approved, in advance, by the Board of Directors, and will be promptly disclosed as required by law or stock exchange regulation.

SOURCE: www.hormel.com/templates/corporate.asp?catitemid=71&id=634, accessed June 14, 2007.

organization's expectations, they realize that fraud hurts the organization, that not everyone is a little dishonest, that the organization won't tolerate dishonest acts, that dishonest behavior is serious, and that unauthorized borrowing is not acceptable.

A second way to create a positive work environment, thus making the organization less vulnerable to fraud, is having open-door or easy access policies. Open-door policies prevent fraud in two ways. First, many people commit fraud because they feel they have no one to talk to. Sometimes, when people keep their problems to themselves, they lose their perspectives about the appropriateness of actions and about the consequences of wrongdoing. This loss of perspective can lead to making decisions to be dishonest. Second, open-door policies allow managers and others to become aware of employees' pressures, problems, and rationalizations. This awareness enables managers to take fraud prevention steps. Studies have shown that most frauds (71 percent in one study) are committed by someone acting alone. Having people to talk to can prevent this type of fraud. One person who had embezzled said, in retrospect, "Talk to someone. Tell someone what you are thinking and what your pressures are. It's definitely not worth it…. It's not worth the consequences."

As an example of a person who committed fraud that probably could have been prevented had the organization had an open-door policy, consider Micky:

> *Micky was the controller for a small fruit-packing company. In that position, he embezzled over $212,000 from the company. When asked why, he said, "Nobody at the company, especially the owners, ever talked to me. They treated me unfairly. They talked down to me. They were rude to me. They deserve everything they got."*

A third way to create a positive work environment, thus making the organization less vulnerable to fraud, is having positive personnel and operating policies. Research has shown that positive personnel and operating policies are important factors in contributing to high- or low-fraud environments. Uncertainty about job security, for example, has been associated with high-fraud environments. Other personnel and operating conditions and procedures that appear to contribute to high-fraud environments include the following:

- *Managers who don't care about or pay attention to honesty (who model apathetic or inappropriate behavior)*
- *Inadequate pay*
- *Lack of recognition for job performance*
- *Imposition of unreasonable budget expectations*
- *Expectations that employees live a certain lifestyle (e.g., belong to a country club)*
- *Perceived inequalities in the organization*
- *Inadequate expense accounts*
- *Autocratic or dictatorial management*
- *Low company loyalty*
- *Short-term business focus*
- *Management by crisis*
- *Rigid rules*
- *Negative feedback and reinforcement*
- *Repression of differences*
- *Poor promotion opportunities*

- *Hostile work environments*
- *High turnover and absenteeism*
- *Cash flow or other financial problems*
- *Reactive rather than proactive management*
- *Managers who model wheeler-dealer, impulsive, insensitive, emotional, or dominant personalities*
- *Rivalrous rather than supportive relationships*
- *Poor training*
- *Lack of clear organizational responsibilities*
- *Poor communication practices*

Each of these conditions or procedures contributes to creating a high-fraud environment. For example, during crisis or rush jobs, there are additional opportunities to commit fraud. When a special project is being hurried toward completion, for example, the normal controls are often set aside or ignored. Signatures are obtained to authorize uncertain purchases. Reimbursements are made rapidly, with little documentation. Record keeping falls behind and cannot be reconstructed. Inventory and supplies come and go rapidly and can easily be manipulated or misplaced. Job lines and responsibilities are not as well defined.

In a recent interview, the controller of a Fortune 500 company indicated that his company had experienced three large frauds in the past year. Two of them, both totaling millions of dollars, had occurred while the company was rushing to complete crash projects.

It would be easy to include many examples of fraud that have been facilitated by each of these high-fraud environmental factors, but we include only two. The first is an example of fraud associated with inadequate pay. The second is an example of fraud associated with the imposition of unreasonable expectations.

A long-time employee of a company believed that he had performed well, but was passed over for a raise he felt he had earned. He was earning $30,000 a year and decided that he was entitled to a 10 percent raise. He stole $250 a month, which was exactly 10 percent of his salary. His moral standards permitted him to steal that much because he felt it was "owed to him," but he could not embezzle one cent more, since that would have been "dishonest."

A division manager of a large conglomerate was told by the company's CEO that he "would" increase his division's segment margin by 20 percent during the coming year. When he realized he could not meet the imposed budget, he overstated revenues. He feared losing his job if he didn't meet his assigned budget.

Implementing Employee Assistance Programs (EAPs)

The third factor in creating a culture of honesty, openness, and assistance is having formal **employee assistance programs (EAPs)**. One of the three elements of the fraud triangle is perceived pressure. Often, fraud-motivating pressures are what perpetrators consider to be unsharable or what they believe have no possible legal solutions. Companies that provide employees with effective ways to deal with personal pressures eliminate many potential frauds. The most common method of assisting employees with pressures is by implementing formal EAPs. EAPs help employees deal with substance abuse (alcohol and drugs); gambling; money management; and health, family, and personal problems.

An EAP that is successfully integrated into an organization's other employee support systems with programs and services that include wellness, team building, coaching, conflict resolution, critical incident response, assessment, counseling, and referral can and does help reduce fraud and other forms of dishonesty. Employees welcome this benefit, they use it, and they report consistently in impact surveys that the EAP made a difference in their lives, and in the quality of their work.

Most successful organizations view EAPs as important contributors to the success of their businesses and as valuable benefits for their employees. Employers are convinced that EAP programs make a difference. Why? Organizations recognize that having the ability to provide a troubled employee with timely and appropriate help results in reducing the financial and human costs associated with an employee who is not fully functioning. Valuable employees have been assisted in dealing successfully with issues that threatened their health, finances, relationships, energy, and ability to contribute strongly in the workplace.[5]

Return on investment (ROI) for EAPs has been studied repeatedly, yet definitive proof of their benefits remains difficult to demonstrate.

As examples of frauds that might have been prevented with EAPs, consider the following two real cases:

An unmarried woman became pregnant. She didn't want her parents or anyone else to know. Needing money desperately, she stole $300 from her company. Then, realizing how easy the theft had been, she stole another $16,000 before being detected.

An employee of a large bank embezzled over $35,000. When she was caught and asked why, she stated that her son was "hooked on heroin at a cost of

nearly $500 per day." Because she could not stand to see him go through withdrawal pains, she had embezzled to support his habit.

> **Remember this …**
>
> *In preventing fraud, it is important to create a culture of honesty, openness, and assistance. Table 4.1 summarizes how to create such a culture.*

Eliminating Opportunities for Fraud to Occur

Earlier in this text, the fraud motivation triangle—perceived pressure, perceived opportunity, and rationalization—was introduced to explain why fraud occurs. When pressure, opportunity, and rationalization combine, the likelihood of a fraud being perpetrated increases dramatically. If one of the three elements is missing, fraud is less likely. In this section, we discuss the second major element in fraud prevention—eliminating opportunities to commit dishonest acts.

In this section, we will cover five methods of eliminating fraud opportunities: (1) having good internal controls, (2) discouraging collusion between employees and customers or vendors and clearly informing vendors and other outside contacts of the company's policies against fraud, (3) monitoring employees and providing a hotline (whistle-blowing system) for anonymous tips, (4) creating an expectation of punishment, and (5) conducting proactive auditing. Each of these methods reduces either the actual or the perceived opportunity to commit fraud, and all of them together combine with the culture factors described earlier to provide a comprehensive fraud prevention program.

Having a Good System of Internal Controls

The most widely recognized way to deter or prevent fraud is by having a good system of controls. The Institute of Internal Auditors' Web site contains the following statement, for example:[6]

> *Internal auditors support management's efforts to establish a culture that embraces ethics, honesty, and integrity. They assist management with the evaluation of internal controls used to detect or mitigate fraud.*

Figure 4.2 shows how organizations assess risks and then implement various controls to minimize those risks.

As stated previously in this text, the Committee of Sponsoring Organizations' (COSO) definition of an *internal control framework* for an organization should include (1) a good control environment, (2) a good accounting system, (3) good control activities, (4) monitoring, and (5) good communication and information. The *control environment* is the overall tone of the organization that management establishes through its modeling and labeling, organization, communication, and other activities. As stated in COSO's report, the control environment sets the tone of an organization,

TABLE 4.1 CREATING A CULTURE OF HONESTY, OPENNESS, AND ASSISTANCE

WAY TO CREATE A CULTURE OF HONESTY, OPENNESS, AND ASSISTANCE	HOW THIS STEP IS ACCOMPLISHED
1. Hire honest people and provide fraud awareness training.	1. Verify all information on the applicant's résumé and application. 2. Require all applicants to affirm the truth of the matters set forth in their application and résumé. 3. Train management to conduct thorough and skillful interviews.
2. Create a positive work environment.	1. Create expectations about honesty by having a good corporate code of conduct and conveying those expectations throughout the organization. 2. Have open-door or easy access policies. 3. Have positive personnel and operating procedures.
3. Provide an employee assistance program (EAP).	1. Implement an EAP that helps employees deal with personal and nonsharable pressures in their lives.

influencing the control consciousness of its people.[7] It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people, management's philosophy and operating style, the way management assigns authority and responsibility and organizes and develops its people, and the attention and direction provided by the board of directors. The control environment also includes well-defined hiring practices, clear organization, and a good internal audit department.

The second element—having a good accounting system—is important so that the information used for decision making and provided to stakeholders is valid, complete, and timely. The system should also provide information that is properly valued, classified, authorized, and summarized.

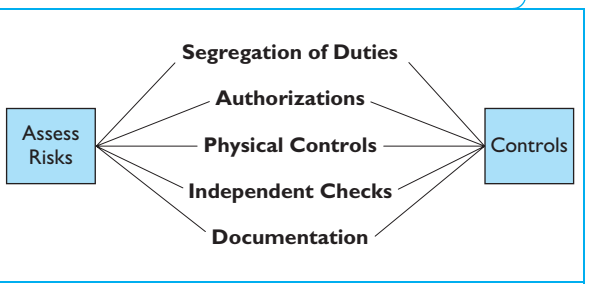
Good control activities involve policies and practices that provide physical control of assets, proper authorizations, segregation of duties, independent checks, and proper documentation. (Physical control, proper authorization, and segregation of duties are controls that usually prevent fraud, thus called preventive controls, while independent checks and documents and records are usually detective controls that provide early fraud detection opportunities.) A control system that meets these requirements provides reasonable assurance that the goals and objectives of the organization will be met and that fraud will be reduced.

Obviously, if a person owns a company and is that company's only employee, not many controls are needed. The owner would not likely steal from the company or serve customers poorly. In organizations with hundreds or thousands of employees or even two or three, controls are needed to ensure that employees behave according to the owner's expectations.

STOP & THINK *It is obvious that controls are important in a business organization to get employees and others to act in a manner consistent with management or the owner's desires. In what other settings would controls be important?*

No internal control structure can ever be completely effective, regardless of the care followed in its design and implementation. Even when an ideal control system is designed, its effectiveness depends on the competency and dependability of the people enforcing it. Consider, for example, an organization that has a policy requiring the dual counting of all incoming cash receipts. If either of the two employees involved in the task fails to understand the instructions, is careless in opening and counting incoming cash, or fails to pay attention to the task at hand, money can easily be stolen or miscounted. One of the employees might decide to understate the count intentionally to cover up a theft of cash. Dual custody can be maintained only if both employees pay full attention to the task and completely understand how it is to be performed.

FIGURE 4.2 ASSESSING RISK AND IMPLEMENTING APPROPRIATE CONTROLS



Because of the inherent limitations of controls, a control system by itself can never provide absolute assurance that all fraud will be prevented. Trying to prevent fraud by having only a good control system is like fighting a skyscraper fire with a garden hose. In combination with the other methods described in the following, however, having a good control framework is an extremely important part of any fraud prevention program.

In determining what kind of control activities an organization should have, it is important to identify the nature of risks involved and the types of abuses that could result from these risks. There are only five types of control activities: (1) segregation of duties—having two people do a task together or splitting the task into parts so that no one person handles the complete assignment; (2) having a system of proper authorizations so that only authorized or designated individuals have permissions to complete certain tasks; (3) implementing physical safeguards such as locks, keys, safes, fences, and so on, to prohibit access to assets and records; (4) implementing a system of independent checks such as job rotations, mandatory vacations, audits, and so on; and (5) having a system of documents and records that provide an audit trail that can be followed to check on suspicious activity and to document transactions. As shown in Table 4.2, the first three are preventive controls, and the last two are detective controls.

TABLE 4.2 TYPES OF CONTROL ACTIVITIES

TYPE OF CONTROL	CONTROL ACTIVITIES
Preventive controls	1. Segregation of duties 2. System of authorizations 3. Physical safeguards
Detective controls	1. Independent checks 2. Documents and records

Once identified and put into place, controls need to be monitored and tested to ensure that they are effective and are being followed. In fact, Section 404 of the Sarbanes-Oxley Act requires all public companies to have their external auditors test their system of internal controls and attest that there are no material weaknesses in the controls.

In determining what kinds of control activities to implement, it is important to assess their costs and benefits. For example, while the most appropriate control from a risk perspective might involve segregation of duties, this control is usually quite expensive. In small businesses with only a few employees, segregation of duties may be too expensive or even impossible. In such cases, it is important to identify less expensive or "compensating" controls that can provide some fraud prevention assurance. For example, in a small service business with eight employees, the owner might personally sign all checks and reconcile all bank statements to control cash.

Often, the problem when fraud is committed is not a lack of controls, but the overriding of existing controls by management or others. Consider the role of controls in the theft of $3.2 million from a small bank—a case that we have discussed previously.

Marjorie, head of accounting and bookkeeping in a small bank, was responsible for all proof reconciliations and activities. Over a seven-year period, she embezzled $3.2 million, or approximately 10 percent of the bank's assets. Auditors and management recognized the lack of segregation of duties in her department, but believed they had compensating controls in place that would prohibit such a theft—that would provide "reasonable assurance" that no fraud was possible in the bank. Some of the compensating controls and the ways they were overridden to allow her fraud were as follows:

1. All deposits and transfers of funds were to be made through tellers. Yet, proof employees were making transfers for bank officers and for themselves. Most people in the bank were aware of this practice, but because it was being done at their boss's request, they didn't think it was wrong.
2. All documents were to be accessible to external auditors. Yet, Marjorie kept a locked cabinet next to her desk, and only she had a key. At one point, a customer whose statement had been altered by Marjorie complained, but was told that he would have to wait until Marjorie returned from vacation because the documentation relating to his account was in Marjorie's locked cabinet.
3. Auditors were supposed to have access to all employees, but Marjorie told her employees not to talk to auditors. Thus, all questions were referred to her during audits.
4. Every employee and every officer of the bank was required to take a two-week consecutive vacation. At Marjorie's request, management allowed this control to be overridden. Based on her memos, that "proof would get behind if she took a two-week vacation," Marjorie was allowed to take her vacation one day at a time. In addition, no one was allowed to perform Marjorie's most sensitive duties while she was away.
5. General ledger tickets were supposed to be approved by an individual other than the person who completed the ticket. To override this control, Marjorie had her employees pre-sign 10 or 12 general ledger tickets, so she wouldn't have to "bother" them when they were busy.
6. There were supposed to be opening and closing procedures of the bank in place to protect the bank, but many employees had all the necessary keys and could enter the bank at will.
7. An effective internal audit function was supposed to be in place. For a period of two years, however, no internal audit reports were issued. Even when the reports were issued, internal audit did not check employee accounts or perform critical control tests, such as surprise openings of the bank's incoming and outgoing cash letters to and from the Federal Reserve.
8. Incoming and outgoing cash letters were supposed to be microfilmed immediately. This compensating control was violated in three ways. First, letters were not usually filmed immediately. Second, for a time, letters were not filmed at all. Third, Marjorie regularly removed items from the cash letters before they were filmed.
9. Employees' accounts were not regularly reviewed by internal audit or by management. On the rare occasions when accounts were reviewed, numerous deposits to and checks drawn on Marjorie's account that exceeded her annual salary were not questioned.
10. Loans were supposed to be made only to employees who met all lending requirements, as if they were

normal customers. At one point, a $170,000 mortgage loan was made by the bank to Marjorie, without any explanation as to how the loan would be repaid or how she could afford such a house.

11. Employees in proof and bookkeeping were not supposed to handle their own bank statements. Yet, employees regularly pulled out their own checks and deposit slips before the statements were mailed.
12. Managers were supposed to be reviewing key daily documents, such as the daily statement of condition, the significant items and major fluctuation report, and the overdraft report. Either managers didn't review these reports, or they didn't pay close attention to them when they did review them. There were daily fluctuations in the statements of condition of over $3 million. The significant items and major fluctuation reports revealed huge deposits to and checks drawn on Marjorie's account. In addition, Marjorie appeared on the overdraft reports 97 times during the first four years she was employed by the bank she defrauded.

If these controls that were supposedly in place had been effective, Marjorie's fraud would have been prevented or at least detected in its early stages. Because management and internal auditors were overriding controls, the bank's "reasonable assurance" provided by internal controls became "no assurance" at all.

Having a good system of internal control is the single most effective tool in preventing and detecting fraud. Unfortunately, sometimes in practice, control procedures are rarely followed the way they are designed or intended. Sometimes, a lack of compliance occurs because employees emulate management's apathetic attitude toward controls. Other times, managers properly model and label good control procedures, but employees do not comply because of disinterest, lack of reward for following or punishment for not following controls, lack of focus, or other reasons. Because control procedures can provide only "reasonable assurance" at best, controls are only one element of a comprehensive fraud prevention plan.

Discouraging Collusion between Employees and Others and Alerting Vendors and Contractors to Company Policies

As stated previously, empirical research has shown that approximately 71 percent of all frauds are committed by individuals acting alone. The remaining 29 percent of frauds—those involving collusion—are usually the most difficult to detect and often involve the largest amounts. Collusive fraud is usually slower to develop (it takes time to get to know others well enough to collude and to "trust" that they will cooperate rather than blow the whistle) than frauds committed by one individual.

Unfortunately, two recent trends in business have probably increased the number of collusive frauds. The first is the increasingly complex nature of business. In complex environments, trusted employees are more likely to operate in isolated or specialized surroundings in which they are separated from other individuals. The second is the increasing frequency of supplier alliances, where oral agreements replace paper trails and closer relationships exist between buyers and suppliers. Certainly, there are increased cost savings and increased productivity from using supplier alliances. How much increased complexity and supplier alliances will cause fraud to increase is still unknown, although most fraud studies show that fraud is increasing every year. Generally, it is the people we "trust" and "have confidence in" who can and do commit most frauds. The reaction of one manager to a recent fraud involving a trusted vendor was, "I just couldn't believe he would do it. It's like realizing your brother is a murderer."

The problem with trusting people—through supplier alliances, and so on—too much is that opportunity and temptation increase. A helpful analogy is that of a company nearly a century ago that was looking for someone to drive its wagons over a rugged mountain.

> *In interviewing prospective drivers, the interviewer asked the first applicant, "How close to the edge of the cliff can you get without going over?" "Why, I can maneuver within six inches without any problems," was the response. When asked the same question, the second interviewee responded, "I can drive within three inches of the edge without going over the cliff." When the third and final applicant was asked, he responded, "I will keep the wagon as far away from the edge as I possibly can, because it is foolish to place yourself in a risky position." Guess which one got the job!*

Fraud is similar to driving wagons over a treacherous road. When risks are higher, there will be more problems. When employees are solely responsible for securing large contracts with vendors, bribes and kickbacks often occur. In some cases, purchasing employees can double or triple their salaries by allowing very small increases in the costs of purchased goods. Purchase and sales frauds are the most common types of collusive frauds. When the opportunity is too high,

even individuals whose professional lives are guided by professional codes of conduct will sometimes commit fraud. Consider the ESM fraud as an example.

In the ESM fraud case, the CPA firm partner accepted under-the-table bribes from his client, in return for staying quiet about fraudulent financial transactions. The fraud being perpetrated by the client exceeded $300 million. The CPA had been the partner-in-charge of the engagement for over eight years. For not disclosing the fraud, the client paid him $150,000. If the CPA firm had not allowed him to be managing partner of the job for such a long time, his participation in the fraud and erosion of integrity would probably have been impossible.

Sometimes otherwise innocent vendors and customers are drawn into frauds by an organization's employees because they fear that if they don't participate, the business relationship will be lost. In most cases, such customers or vendors have only one or two contacts with the firm. They are often intimidated by the person who requests illegal gratuities or suggests other types of inappropriate behavior. A periodic letter to vendors that explains an organization's policy of not allowing employees to accept gifts or gratuities helps vendors understand whether buyers and sellers are acting in accordance with the organization's rules. Such letters clarify expectations, which is very important in preventing fraud. Many frauds have been uncovered when, after such a letter was sent, vendors expressed concern about their buying or selling relationships.

A large chicken fast-food restaurant discovered a $200,000 fraud involving kickbacks from suppliers. After investigating the fraud, the restaurant management decided to write letters to all vendors explaining that it was against company policy for buyers to accept any form of gratuities from suppliers. The result of the letters was the discovery of two additional buyer-related frauds.

A related precaution that is often effective in discouraging collusive-type frauds is printing a "right-to-audit" clause on the back of all purchase invoices. Such a clause alerts vendors that the company reserves the right to audit their books any time. Vendors who know that their records are subject to audit are generally more reluctant to make improper payments than those who believe their records are confidential and will never be examined. A right-to-audit clause is also a valuable tool when conducting fraud investigations.

Monitoring Employees and Having a Whistle-Blowing System

Individuals who commit fraud and hoard stolen proceeds are virtually nonexistent. Almost always, perpetrators use their stolen money to support habits, increase their lifestyle, or pay for expenses already incurred. When managers and their colleagues pay close attention to lifestyle symptoms resulting from these expenditures, fraud can often be detected early. Most stolen funds are spent in conspicuous ways. Fraud perpetrators usually buy automobiles, expensive clothes, or new homes; take extravagant vacations; purchase expensive recreational toys, such as boats, condominiums, motor homes, or airplanes; support extramarital relationships or outside business interests. Consider again the case of Marjorie, our previously discussed bank proof operator:

Marjorie first started working for the bank in 1980. During her first four years of employment, she took out a debt consolidation loan of approximately $12,000 and had 97 personal overdrafts. During the next seven years, while committing fraud, her salary never exceeded $22,000 per year. Yet, colleagues and officers of the bank knew that she had done the following:

- Taken several expensive cruises
- Built a home on a golf course, costing over $600,000
- Purchased and was currently driving the following cars:
  Rolls Royce
  Jeep Cherokee
  Audi
  Maserati
- Purchased the following personal items:
  Expensive jewelry, including 16 diamonds and sapphires
  Computers
  Stereos
  VCRs
  Electronic gear
  Snowmobiles
  Golf cart
  Expensive gifts for colleagues and relatives
  Fur coat
  Tanning bed
  Expensive clothes
- Taken limousines several events
- Held extravagant parties for employees and others at her home
- Bought a condominium for her mother-in-law
- Purchased a glass art collection costing over $1.5 million
- Taken domestic trips to buy glass art
- Had her home extravagantly remodeled

Anyone paying attention would have realized that Marjorie's lifestyle was inconsistent with her level of earnings. When a coworker finally asked her how she could afford everything, she explained that her husband had received a one-third inheritance of $250,000. The story wasn't true, but even if it had been, the $83,333 that her husband had supposedly inherited wouldn't have paid for the Maserati, let alone all the other luxuries that managers knew she had purchased.

Close monitoring facilitates early detection. It also deters frauds because potential perpetrators realize that "others are watching." It is because monitoring by colleagues is such an effective way to catch dishonest acts that Section 307 of the Sarbanes-Oxley Act of 2002 requires all public companies to have a whistleblower system that makes it easy for employees and others to report suspicious activities.

In most cases of fraud we have studied, individuals suspected or knew that fraud was occurring but were either afraid to come forward with information or didn't know how to reveal the information. The new whistle-blowing laws should help in these cases.

Even with advances in technology, the most common way in which fraud is detected is through tips. In one empirical study, for example, the authors found that 33 percent of all frauds were detected through tips, while only 18 percent were detected by auditors. A company that experienced over 1,000 frauds in one year determined that 42 percent were discovered through tips and complaints from employees and customers. A good whistle-blowing program is one of the most effective fraud prevention tools. When employees know that colleagues have an easy, nonobligatory way to monitor each other and report suspected fraud, they are more reluctant to become involved in dishonest acts.

Deloitte, one of the Big 4 CPA firms, in a worldwide study it conducted, concluded that there were four reasons why some whistle-blowing systems fail in their attempts to detect misconduct.[8]

1. **Lack of anonymity**—One of the biggest impediments for whistle-blowers to report misconduct is the fear of retribution. If employees have to report misconduct through an internal channel that doesn't guarantee anonymity, they are less likely to "blow the whistle." They want to alert their organization to misconduct but not at a personal expense.
2. **Culture**—An organization's culture is set by the tone at the top. If management sets a poor example regarding misconduct, employees are less likely to speak out for two reasons: first they fear being chastised by management; and second, they believe that management is unlikely to act on a whistleblower's report, especially if it relates to the management team.
3. **Policies**—If policies in relation to acceptable behavior and ethics are not abundantly clear within an organization, employees will be uncertain about what constitutes misconduct and whether or not to report suspicious activity.
4. **Lack of awareness**—If the existence of the whistleblowing system is not communicated effectively or continually reinforced, employees are less likely to use it or know how to access it.

Consistent with these findings, research has shown that for a whistle-blowing system to work effectively, it must have the following elements:

1. **Anonymity**—Employees must be assured that they can report suspected incidents of misconduct without fear of retribution. An effective system must conceal the identity of a whistle-blower. While this may lead to a proportion of mischievous reports, these can be easily verified through a follow-up investigation of reported incidents.
2. **Independence**—Employees feel more comfortable about reporting misconduct to an independent party that is not in any way related to the organization or the party or parties involved in the misconduct.
3. **Accessibility**—Employees must have several different channels through which they can report misconduct, that is, via the telephone, e-mail, online, or mail. This ensures that all employees—entry-level, managers on-site, off-site—can anonymously make a report using the channel that suits them.
4. **Follow up**—Incidents reported through the whistleblowing system must be followed up and corrective action must be taken where necessary. This will demonstrate the benefit of the system and encourage further reporting of misconduct.

It is not only companies in the United States that have whistle-blowing systems but also government agencies and foreign companies in major countries including Korea. The following was taken from the Web site of Toshiba, a Japanese company:

> *Toshiba introduced the Risk Hotline, a whistleblower system, in January 2000. Using the system, employees can report their concerns or seek advice via the intranet so that Toshiba can find risks in advance and preclude breach of compliance. Further*

improvements have been made to the whistle-blower system. Since January 2005, it has been possible to contact an outside attorney in addition to the Legal Affairs Division, thereby strengthening the reliability and the transparency of the system and its convenience for whistle-blowers.

In response to the Whistle-Blower Protection Act of Japan which came into force in April 2006, all Toshiba Group companies in Japan have implemented whistle-blower systems and a growing number of Group companies overseas have adopted such systems. Similar to Toshiba Corporation, major Group companies in Japan have enhanced their whistle-blower systems by setting up direct links to outside attorneys.

Pursuant to the Whistle-Blower Protection Act of Japan, whistle-blowers among employees of suppliers/partners who report concerns about a company are also granted protection from disadvantageous treatment. Therefore, Toshiba introduced the Clean Partner Line in Japan, a whistle-blower system for suppliers/partners.[9]

Creating an Expectation of Punishment

The fourth factor in eliminating fraud opportunities is creating an expectation that dishonesty will be punished. As stated several times, one of the greatest deterrents to dishonesty is fear of punishment. In today's business and social environment, merely being terminated is not meaningful punishment. Real punishment involves having to tell family members and friends about the dishonest behavior. Fraud perpetrators are usually first-time offenders who suffer tremendous embarrassment when they are forced to inform their loved ones that they have committed fraud and been caught. When fraud perpetrators are merely terminated, they usually give those close to them a morally acceptable, but false, reason for the termination, such as, "the company laid me off," "the company is downsizing," or "I just can't stand working there any more."

A strong prosecution policy that is well publicized lets employees know that dishonest acts will be harshly punished, that not everyone is dishonest, and that unauthorized borrowing from the company will not be tolerated. While investigation and prosecution are often expensive and time consuming, and while pursuing legal action stimulates concerns about unfavorable press coverage, not prosecuting is a cost-effective strategy only in the short run. In the long run, failure to take legal action sends a message to other employees that fraud is tolerated and that the worst thing that happens to perpetrators is termination. Because of today's privacy laws and high job turnover rates, termination alone is not a strong fraud deterrent. Like a good code of ethics that conveys expectations, a strong policy of punishment helps eliminate rationalizations. Some people believe the reason there is so much fraud and white-collar crime is that perpetrators are not usually punished and, when they are, the punishments are light.

Conducting Proactive Fraud Auditing

Very few organizations actively audit for fraud. Rather, their auditors are content to conduct financial, operational, and compliance audits and to investigate fraud only when symptoms are so egregious that fraud is suspected. Organizations that proactively audit for fraud create awareness among employees that employees' actions are subject to review at any time. By increasing the fear of getting caught, proactive auditing reduces fraudulent behavior.

As will be discussed in Chapter 5, good fraud auditing involves four steps: (1) identifying fraud risk exposures, (2) identifying the fraud symptoms of each exposure, (3) building audit programs to proactively look for symptoms and exposures, and (4) investigating fraud symptoms identified. One company, for example, decided to use proactive computer auditing techniques to compare employees' telephone numbers with vendors' telephone numbers. The search revealed 1,117 instances in which telephone numbers matched, indicating that the company was purchasing goods and services from employees—a direct conflict of interest.

Even CPA firms have become very serious about proactively auditing for fraud. Part of this motivation comes from Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit*. SAS No. 99 includes sections dealing with brainstorming the risks of fraud while emphasizing increased professional skepticism; discussions with management and others as to whether or not they are aware of fraud or fraud symptoms; the use of unpredictable audit tests; and responding to management override of controls by requiring on every audit certain procedures responsive to detecting management override.

SAS No. 99 was issued because the Auditing Standards Board [which has now been replaced by the Public Company Accounting Oversight Board (PCAOB)] believes that by forcing auditors to explicitly consider and brainstorm about fraud, the likelihood that auditors will detect material misstatements due to fraud in a financial statement audit will be increased.

In addition to being more skeptical in their auditing of financial statements, large CPA and other firms have developed dedicated units that specialize in proactively detecting fraud. With advances in technology, the proactive detection of fraud is now possible more than ever before. The use of technology to proactively detect fraud will be addressed in Chapter 6. For now, you only need to know that proactive fraud detection cannot only catch frauds that are occurring early, but it can also serve as a powerful deterrent when employees and others know that an organization is always searching for fraud that may be occurring.

Remember this …

The five methods of eliminating fraud opportunities are (1) having good internal controls, (2) discouraging collusion between employees and customers or vendors and clearly informing vendors and other outside contacts of the company's policies against fraud, (3) monitoring employees and providing a hotline (whistle-blowing system) for anonymous tips, (4) creating an expectation of punishment, and (5) conducting proactive auditing. When fraud opportunities are eliminated or seriously curtailed, it takes more pressure and rationalization for fraud to be committed.

Preventing Fraud—A Summary

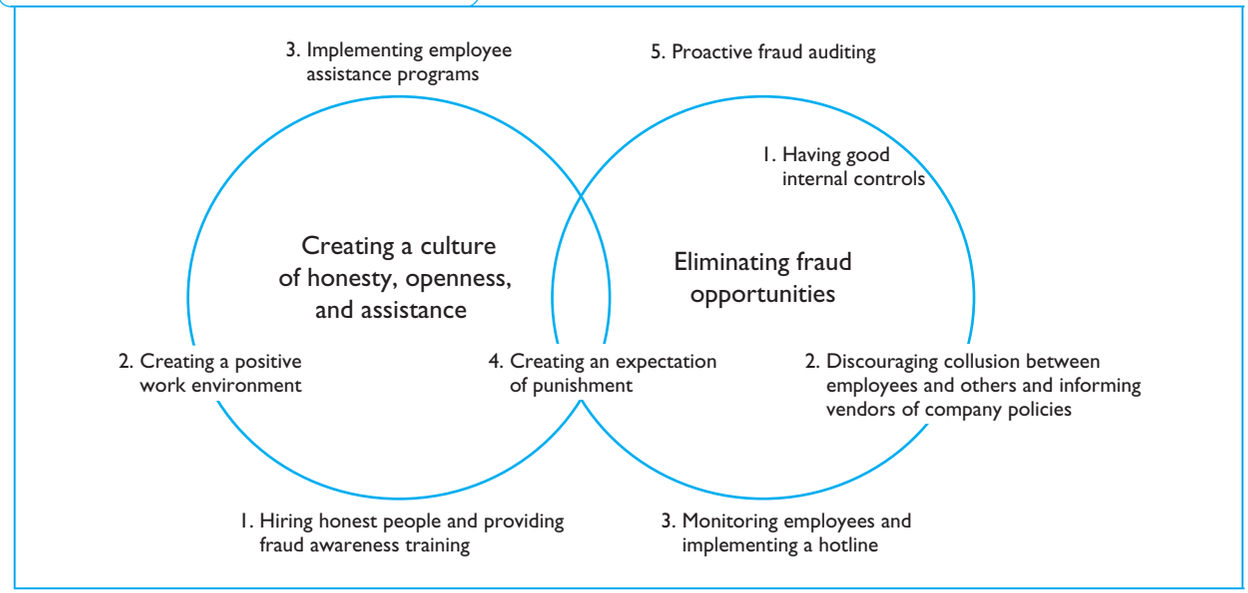
Thus far in this chapter, we have stated that fraud is reduced and prevented by (1) creating a culture of honesty, openness, and assistance and (2) eliminating fraud opportunities. These two fraud prevention activities, together with their sub-elements, are shown in Figure 4.3.

Organizations that employ these steps and techniques have significantly fewer fraud problems than those that don't. One company that worked hard at implementing these steps reduced known fraud from an average of more than $20 million per year to less than $1 million per year.

A Comprehensive Approach to Fighting Fraud

Until now, this chapter has focused only on preventing fraud. We will also combine prevention with detection, investigation, and follow-up to consider a comprehensive approach to fighting fraud. As mentioned earlier, the authors conducted a study that involved surveying Fortune 500 companies about fraud. Questionnaires were sent to each of the 500 companies, with instructions that the individual in the company who was most responsible for fraud prevention should respond. Of the 242 responses, 62 percent (150 responses) came from directors of internal audit, 28 percent (67

FIGURE 4.3 FRAUD PREVENTION



responses) from directors of corporate security, and 10 percent (25 responses) from personnel or human resource directors. Many respondents wrote that their organization had no one person who was "most responsible for fraud prevention," but that they personally were taking responsibility for completing the questionnaire.

The diversity in the job titles of respondents, combined with comments that no one in the organization was primarily responsible for preventing fraud, is a discouraging commentary on the status of fraud prevention in the United States. Fraud is an extremely costly problem for organizations. Yet, responsibility for fraud in an organization is often seen as belonging to "someone else." Independent auditors maintain they can't detect fraud because it isn't their responsibility and because their materiality levels are too high.[10] Internal auditors usually stress that their functions are to evaluate controls and to improve operational efficiency. If they happen to find fraud, they'll pursue or report it, but fraud prevention and detection isn't their primary responsibility. Corporate security officers, in most organizations, believe that theirs is an investigative role and that they will pursue reported frauds. They don't envision their role as including prevention or detection. Managers usually perceive running the business as their responsibility and seldom even acknowledge the possibility that fraud could occur in their organization. Fraud, to them, is something that happens in "other organizations." Further, they don't know how to handle fraud situations that do occur. Employees who are usually in the best position to prevent and detect fraud often don't know what to do or whom to talk to when they have suspicions, and they also often feel that it is unethical or unwise to blow the whistle or report colleagues.

Because this "non-ownership" attitude regarding fraud is prevalent in most businesses, frauds like the one described below will continue to occur.

Jerry Watkins had been working for Ackroyd Airlines for 17 years. During this time, he held several positions in accounting, finance, and purchasing. Jerry was the father of three children, two boys and one girl. Over the years, Jerry and his family had been active in the community and in their church. Jerry coached both Little League baseball and football. He and his wife, Jill, both had college degrees, both worked full time, and both had a long-term goal of sending their children to college. Despite their plans for college, each year the Watkins spent most of what they made and saved very little for college tuition and other expenses.

After Jerry had been working at Ackroyd for 15 years, Steve (Jerry and Jill's oldest son) attended college at a well-known Ivy League university. He performed well, and both Jerry and Jill were proud of Steve's and their other children's accomplishments. Approximately a year later, Jerry, who handled all the family finances, realized they could no longer pay Steve's college expenses, let alone pay future college expenses for their other two children. Jerry, a proud man, could not bring himself to admit his financial inadequacy to his family. He already had a large mortgage and several credit card and other debts, and he knew he could not borrow the money needed for college.

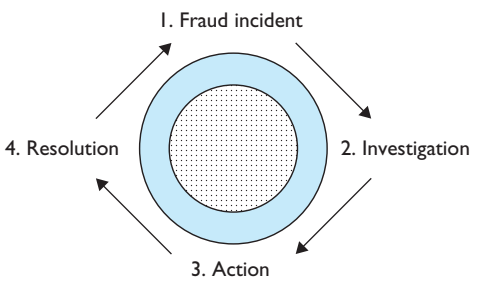
Because of his financial predicament, Jerry decided to embezzle money from Ackroyd Airlines. He had heard of several other thefts in the company, and none of the perpetrators had been prosecuted. In fact, the frauds that he knew about had resulted in the company merely transferring the employees. In addition, Jerry rationalized that he would pay the money back in the future. In his current position as purchasing manager, he found it easy to take kickbacks from a vendor who had previously approached him with favors to get business. At first, Jerry took only small amounts. As the kickbacks proceeded, however, he found that he increasingly relied on the extra money to meet all kinds of financial "needs" in addition to college expenses. He felt guilty about the kickbacks but knew that the company auditors never thought about fraud as a possibility. Anyway, he felt the company would understand if they knew how badly he needed the money. Significant good was coming from his "borrowing." His children were getting an education they could otherwise not have afforded, and Ackroyd didn't really miss the money. Because of his pressure, his opportunity, his rationalization, and Ackroyd's inattention to fraud prevention and detection, the company's honest employee of 17 years stole several hundred thousand dollars.

What is alarming is that Jerry's case is not unusual. Jerry had never signed a code of conduct. Ackroyd's auditors had never proactively searched for fraud. The company didn't have an EAP to help employees with financial and other needs. Furthermore, as Jerry was well aware, the company had never taken actions harsher than terminating previous fraud offenders.

Organizations and Fraud—The Current Model

Like Ackroyd Airlines, many organizations do not have a proactive approach to dealing with fraud and reducing fraudulent behavior. Since fraud prevention is not emphasized in many companies, there is significant confusion about who has responsibility for the

FIGURE 4.4 DEALING WITH FRAUD: THE CURRENT (DEFAULT) MODEL



detection, prevention, and investigation of fraud. The current model that most organizations typically use for dealing with fraud, often by default, is shown in Figure 4.4.[11]

This model is characterized by four stages. In Stage 1, a fraud incident occurs in an organization. This fraud incident is not preceded by formal awareness training or other prevention measures. Once the incident occurs, the firm shifts into a crisis mode, because it (a) needs to identify the perpetrator, (b) wants to avoid publicity, (c) wants to attempt to recover the losses, (d) wants to minimize the overall impact of the occurrence on the organization, and (e) is caught up in the emotion of the crisis.

Stage 2 is investigation. Here security and internal audit usually become involved. Most of the investigative work involves interviewing and document examination. Investigation may or may not lead to resolution, can take extensive time, and may be relatively costly.

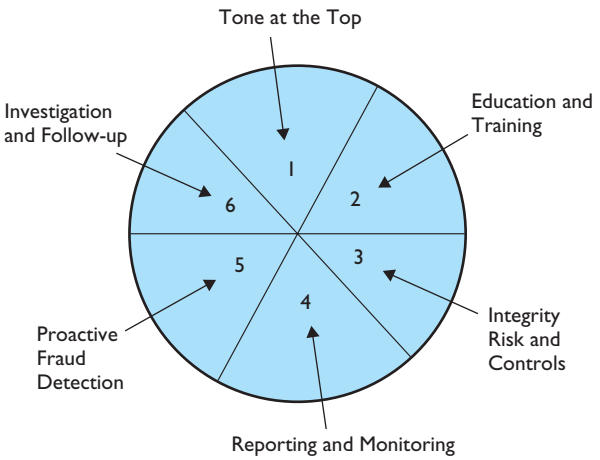
In Stage 3, after the investigation has been completed, the company must decide what actions to take regarding the perpetrator(s). The choices are (a) take no action, (b) terminate or transfer only, or (c) terminate and seek prosecution.

Stage 4 involves closing the file, tying together loose ends, replacing the employee (obviously incurring additional costs), perhaps implementing some new controls, and otherwise resolving the problem. Once these four stages are completed, no further action is taken—until another fraud occurs. Unfortunately, with this model, fraud will never decrease. Instead, it will become a recurring problem. A much better approach to fighting fraud is the one depicted in Figure 4.5.

As you can see, there are six elements included in the fraud-fighting model. First and probably most important is having management, the board of directors, and others at the top of an organization set a positive "tone at the top." Creating a positive tone involves two steps: (1) caring enough about having a positive organization that effective fraud teaching and training is conducted throughout the organization and a well-defined corporate code of conduct is promoted and (2) setting a proper example or modeling appropriate management behavior.

When the management of one company changed its attitude from "we want to know when someone who commits fraud is prosecuted" to "we want to know

FIGURE 4.5 SOUND ORGANIZATIONS—MINIMAL FRAUD



when someone who commits fraud *isn't* prosecuted" and made fraud against the company, along with safety, discrimination, and substance abuse, significant issues in the organization, the number and size of frauds decreased substantially. Likewise, top management cannot accept expensive perks and gifts from vendors and others and not expect employees to do the same.

The second element in this fraud-fighting model is educating employees and others about the seriousness of fraud and informing them what to do if fraud is suspected. As we have repeatedly said, it is fraud prevention, not detection or investigation, that results in big savings. Therefore, significant attention should be given to instituting proactive fraud education initiatives, rather than to dealing with losses that have already occurred.

Fraud awareness training helps to prevent fraud and ensure that frauds that do occur are detected at early stages, thus limiting financial exposure to the corporation and minimizing the negative impact on the work environment. Education includes instructing vendors and other outsiders, not just employees, about the organization's expectations.

The third fraud-fighting element involves integrity risk assessment and having a good internal control system. We have already discussed internal controls in this chapter. It is important to note that having a good system of controls means that there will be an explicit study of all frauds and why they occurred, together with implementation of control activities necessary to prevent future occurrences of the same types of frauds in the future.

Analysis of frauds involves determinations by people in management, audit, security, human resources, control, and finance of why and how the fraud occurred. The focus is on the individuals who were involved, the controls that were compromised or absent, the environment that facilitated the fraud, and related factors. This step is important in understanding the kinds of preventive measures that are needed within the environment in which the fraud occurred. An appropriate preventive solution does not take long to be developed, once all the parties work together to resolve the problems. Obviously, additional or new controls must meet the cost-effectiveness test and may not be implemented. The decision not to implement, however, should be based on an analysis of costs and benefits. They should not be made by default because the proper analysis was not conducted.

The fourth element includes having a system of reporting and monitoring. Fraud reporting must be facilitated. With murder, bank robbery, or assault, there is usually no question about whether a crime has been committed. Fraud, however, is a subtle crime, for which there are usually no obvious signs. Only fraud symptoms or red flags are observed. Because hotlines or other reporting systems often don't exist, employees rarely volunteer information about possible fraud symptoms. This lack of reporting is unfortunate, because employees are in the best position to recognize dishonest behavior or to question red flags with which they are more familiar than anyone else. Monitoring involves having internal auditors, external auditors, and even management performing audits and reviews. Employees and vendors who know that an effective monitoring and reporting system is in place are much less likely to commit fraud than are individuals who work in high fraud environments. Effective prevention of fraud usually involves efforts to create in the minds of potential perpetrators that their activities will be uncovered. For prevention purposes, it doesn't really matter whether a perpetrator actually will be caught, but rather only whether he or she thinks they will.

Reporting also involves publishing facts about the fraud to those who can benefit from the information. Publication does not mean making sure the case and all its accompanying details are in local newspapers. Indeed, until there is a conviction, such publication is ill-advised, because it can lead to slander or libel suits. Rather, what "publication" means in this context is depersonalizing the case (that is, disguising the identities of the perpetrators and other people involved) and publishing it internally in a security newsletter or a memo that is distributed to auditors, security personnel, and appropriate management and employees. Even generic publication of fraud has a tremendous impact, because it helps readers understand that fraud happens in their own organization and is not just a horrible nightmare that occurs elsewhere.

The fifth element of a good fraud-fighting system involves having proactive fraud detection methods in place. No matter how good fraud prevention efforts are, some frauds will still be committed. And, since frauds grow geometrically over time, it is important to detect frauds early. Proactive fraud detection methods, such as those discussed in Chapter 5, are not only effective in detecting fraud, but knowledge of their use is a good fraud deterrent.

The final element involves having effective investigation and follow-up when fraud occurs. Effective

investigation means an organization will have prespecified formal fraud policies stating who will carry out all elements of an investigation. The investigation procedures must be well established, including (a) who will conduct the investigation; (b) how the matter will be communicated to management; (c) whether and when law enforcement officials will be contacted; (d) who will determine the scope of investigation; (e) who will determine the investigation methods; (f) who will follow up on tips of suspected fraud; (g) who will conduct interviews, review documents, and perform other investigation steps; and (h) who will ultimately determine the corporate response to fraud, disciplines, control, and so on. This stage also involves having preset policies regarding follow-up actions against perpetrators.

Taking no action should not even be a possibility; rather, whenever possible, fraud perpetrators should be prosecuted. A strong prosecution policy must have the support of top managers, and they must be informed if someone commits fraud and is not prosecuted. Gone are the days when prosecution resulted in bad publicity. Most people now realize that fraud exists in every organization. They also realize that organizations that take a tough prosecution stance will reduce the number of future frauds significantly and will ultimately be more profitable because of the deterrent effect of prosecution.

As stated previously, the single greatest factor in deterring dishonest acts is the fear of punishment. Companies with successful prosecution policies have developed their own internal investigation experts. They recognize that in order to obtain cooperation from law enforcement officers and the justice system, it is almost always necessary to conduct a thorough and complete investigation (usually including obtaining a signed confession) before the overworked law enforcement agencies and criminal justice systems can accommodate the prosecution.

Remember this …

Every organization will have some fraud. The amount of fraud different organizations have will depend on what kind of training and education they provide, the tone at the top of the organization, how good their risk assessment and internal controls are, what kind of proactive fraud detection programs they have in place, and how they investigate and follow up on frauds that do occur.

Review of the Learning Objectives

- **Understand how to create a culture of honesty, openness, and assistance**. Creating a culture of honesty, openness, and assistance includes three factors: (1) hiring honest people and providing fraud awareness training; (2) creating a positive work environment, which means having a well-defined code of conduct, having an open-door policy, not operating on a crisis basis, and having a low-fraud atmosphere; and (3) providing an employee assistance program that helps employees deal with personal pressures.
- **Know how to eliminate opportunities for fraud**. The five ways to eliminate fraud opportunities are (1) having good internal controls, (2) discouraging collusion between employees and customers or vendors and clearly informing vendors and other outside contacts of the company's policies against fraud, (3) monitoring employees and providing a hotline (whistle-blowing system) for anonymous tips, (4) creating an expectation of punishment, and (5) conducting proactive auditing. Most organizations try to eliminate fraud opportunities by having a good system of internal controls.
- **Understand how to create an effective organization to minimize fraud**. Most organizations do not have a comprehensive approach to preventing and deterring fraud. In fact, most companies don't think about fraud until they experience one. When fraud occurs, they go into crisis mode, investigate and try to resolve the fraud, and then wait until another fraud occurs. A much more comprehensive fraud-fighting approach would involve (1) creating the right kind of modeling and tone at the top, (2) educating and training employees about fraud, (3) assessing risks and putting proper controls in place, (4) having reporting and monitoring systems in place, (5) proactively auditing for fraud and then, when fraud does occur, (6) investigating and following up on the fraud.
- **Understand the importance of proactive fraud auditing.** Very few organizations actively audit for fraud. Rather, their auditors are content to conduct financial, operational, and compliance audits and to investigate fraud only when symptoms are so egregious that fraud is suspected. Organizations that proactively audit for fraud create awareness among employees that their actions are subject to review at

any time. By increasing the fear of getting caught, proactive auditing reduces fraudulent behavior.

- **Understand the importance of creating a comprehensive approach to fighting fraud.** In order to minimize fraud, organizations should combine fraud prevention with fraud detection efforts as well as investigation and follow-up efforts to create a comprehensive approach to fighting fraud. By doing so, organizations can create a synergistic approach that reduces fraud and creates a positive work environment.

KEY TERMS

Employee Assistance Programs (EAPs), p. 112

QUESTIONS

Discussion Questions

1. How do organizations create a culture of honesty, openness, and assistance?
2. What are different ways in which companies can eliminate opportunities for fraud?
3. What is the purpose of adopting a code of ethics throughout a company?
4. Why are good internal controls important?
5. In what ways can organizations discourage collusive fraud?
6. Why is it important to inform outside vendors of company policies concerning payments to buyers?
7. How can organizations monitor their employees?
8. In what ways can organizations conduct proactive fraud auditing?
9. How does a response hotline for anonymous tips help to prevent fraud?
10. What is implied by the phrase "just about everyone can be dishonest"?
11. What are some nonstandard ways of trying to detect dishonest employees in the employee hiring process?
12. How does the Pygmalion effect relate to fraud prevention?

True/False

1. Even with the right opportunity or significant pressure, most people would probably not steal or embezzle.
2. Studies show that a positive and honest work culture in a company does little to prevent fraud.
3. An important factor in creating a culture of honesty, openness, and assistance in the workplace is maintaining an employee assistance program.
4. A good internal control system within a company can ensure the absence of fraud.
5. When fraud is committed, the problem is often not a lack of controls, but the overriding of existing controls by management and others.
6. The two elements in creating a positive work environment are (1) having an open-door policy and (2) having positive personnel and operating procedures.
7. Not prosecuting fraud perpetrators is cost effective both in the short run and the long run.
8. Even a good system of internal controls will often not be completely effective because of fallibilities of the people applying and enforcing the controls.
9. The increasingly complex nature of business helps to decrease the number of collusive frauds.
10. Tips and complaints are the most common way fraud is detected.
11. The major role of employee assistance programs is to help employees recover from the damaging psychological effects of fraud.
12. Not all possible controls should be implemented; rather, one must assess a control's cost and benefits before implementation.
13. Creating an expectation of punishment causes firm morale to deteriorate and often results in lower productivity.

Multiple Choice

1. People will often be dishonest if they are placed in an environment of:
   a. Poor controls.
   b. High pressure.
   c. Low integrity.
   d. Loose accountability.
   e. All of the above.
2. Which of the following factors contribute to creating a corporate culture of honesty and openness?
   a. Hiring honest people.
   b. Performing criminal background checks.
   c. Not having an open-door policy.
   d. Having a well-understood and respected code of ethics.
   e. Both a and d.
   f. All of the above.

3. Which of the following personnel and operating policies contribute to high-fraud environments?
   a. Management by crisis.
   b. Rigid rules.
   c. High employee lifestyle expectations.
   d. Poor promotion opportunities.
   e. All of the above.
4. The single most effective tool in preventing and detecting fraud is usually:
   a. Monitoring employees.
   b. Having a good system of internal controls.
   c. Having a well-written company code of ethics.
   d. Following strict hiring procedures.
5. A company's control environment includes:
   a. The tone that management establishes toward what is honest and acceptable behavior.
   b. Corporate hiring practices.
   c. Having an internal audit department.
   d. All of the above.
6. Which of the following factors generally results in a high-fraud environment?
   a. Hiring honest people.
   b. Providing an EAP.
   c. Autocratic management.
   d. Both a and b.
7. Which of the following aspects of fraud usually results in the largest savings?
   a. Fraud prevention.
   b. Fraud detection.
   c. Fraud investigation.
   d. It is impossible to tell.
8. Which of the following is usually the most effective tool in preventing and detecting fraud?
   a. Discouraging collusion between employees and customers or vendors.
   b. Effective investigations of fraud symptoms.
   c. Having a good system of internal controls.
   d. Creating an expectation of punishment in the company.
9. Which of the following is the typical fraud model that describes most firms?
   a. Fraud incident, assessing risk, investigation, reporting.
   b. Fraud incident, investigation, action, resolution.
   c. Assessing risk, fraud incident, investigation, resolution.
   d. Assessing risk, investigation, implementing a fraud program, reporting.
10. The "tone at the top" is an important element in fighting fraud which involves:
    a. Doing a good job of integrity risk assessment.
    b. Having a positive organization where effective fraud teaching and training is conducted.
    c. Setting a proper example or modeling appropriate management behavior.
    d. Both b and c.
11. Which of the following is *not* a recognized method of eliminating fraud opportunities?
    a. Having good internal controls.
    b. Monitoring employees.
    c. Creating an expectation of punishment.
    d. Engendering employee goodwill by having lax rules.
12. Which of the following is *not* a reason identified by Deloitte why whistle-blowing systems fail?
    a. Lack of anonymity.
    b. Pressure to comply.
    c. Culture.
    d. Lack of awareness.
13. Alerting vendors and contractors to company policies often results in:
    a. Loss of interest in the organization by vendors.
    b. Discovery of current frauds and the prevention of future frauds.
    c. Strained vendor/purchaser relationships.
    d. Heightened incidence of recurrent reverse-vendor fraud.

SHORT CASES

Case 1

Karen, a friend of yours, recently started her own business, The Bike and Boulder Company (B&B). B&B specializes in the sales of mountain bikes and rock-climbing equipment. Karen is putting the finishing touches on her company policies and procedures. She knows you are taking a fraud class and asks you to review what she has completed thus far. You quickly notice that Karen has neglected to address fraud and fraud prevention in her policies and procedures. What policies and procedures would you suggest Karen implement to prevent and detect fraud at B&B?

Case 2

Because ABC Company suffered large losses from fraud last year, senior management has decided to be more proactive in implementing a fraud prevention environment. In interviewing employees, they found that many employees were unclear about which

behaviors were ethical and which were not. What could management do to better educate employees about ethical behavior?

Case 3

Jason works at a new software development company. The company has been in existence for only two years. Since the company is new, everybody is working extra hours and spending all of their time developing new products that can be sold to customers. Everybody is busy, and there is very little time for manager–employee interviews. The culture of the company is trusting and fun. When Jason started with the company, the only agreement he had to sign was an agreement to not transfer company software secrets to other organizations. Earlier in the year, Jason learned of an instance where another employee in accounting was fired. The reason was rumored to be fraudulent behavior, but nobody really knew the reason. Do the company's operating procedures encourage fraudulent behavior? In what ways?

Case 4

Nellie works for a large Fortune 500 company. She heads the information systems department and works closely with the accounting department. The company works with many associates. They have many buyer and supplier companies they work with. Nellie knows a lot about the database systems and accounting practices in the company. She even works closely with buyers and suppliers to create data communication lines. Recently, Nellie has become concerned about the integrity and reliability of the accounting and information systems. The company has grown to a point where she cannot manage or supervise all the activities performed in these areas. What proactive steps can Nellie take to ensure systems and accounting integrity and prevent fraudulent behavior?

Case 5

While performing an audit of TCC Corporation, the audit team noticed something that didn't look right. The company's receivables aging report showed that bank loan eligible receivables were approximately $91 million. The audit team calculated the bank loan eligible receivables to be approximately $50 million. The client didn't identify specific accounts in writing off bad debts, there was extremely slow credit memo processing, and items that management had not focused on remained uncollectible and ineligible for financing. In addition, over the last two years, the company's credit department has had unusually high turnover—four different people had held the credit manager position under an intimidating CFO. The current credit manager was a friend of the CFO and had worked with him at a previous company. After looking at some invoices and asking about customer information to confirm, the credit manager admitted to creating false documents and arranging fictitious sales with clients—all with the knowledge of the CFO.

1. What are some of the red flags that point to the possibility of fraud?
2. What would you say was the main problem in this case that allowed the fraud to occur?

Case 6

Joseph Gonzales recently bought a new business that included a small 20-room motel and coffee shop. He hired a young couple to run the business and plans to pay them a monthly salary. The couple will live for free in a small apartment behind the motel office and will be in charge of the daily operations of the motel and coffee shop. They will also be responsible for hiring and supervising the four or five part-time employees who will help with cleaning the rooms, cooking, and waiting on customers in the restaurant. The couple will also maintain records of rooms rented, meals served, and payments received (which can be in the form of cash, checks, or credit cards). They will make weekly deposits of the business's proceeds at the local bank. Joseph lives about six hours away and will only be able to visit periodically.

1. What are your two biggest concerns about possible fraud on the part of the couple?
2. For each concern, identify a possible control that could reduce the risk of fraud.

Case 7

Danny has been working at Gant Automobile for two years. He feels fortunate to have held his job for so long, considering his past, which involved being fired for fraudulent activities in two different cases. His boss, Mr. Gant, is generally a pretty cold person and only says hello to Danny upon arriving and leaving work each day. All of the guys at work tend to slack a little here and there. They don't mind eating lunch at the company's expense, and there is a general lack of order about the place. Danny has been feeling tight on cash lately, having just moved into a home that is perhaps a little too expensive. With this internal pressure and no one on whom to unload his troubles or with whom to talk, Danny decides to steal parts from the parts garage

and sell them on the street for cash. What could Gant Automobile have done to prevent Danny's fraud?

Case 8

Mary is the owner of a small flower shop. With only 12 employees, the environment is one of trust. Mary personally knows each employee, and most have worked at the shop since its opening. Although few controls exist, Mary is the only person allowed to sign checks. Mary's good friend, Steve, is very important to the business. Not only is he the head accountant, but he also helps maintain relationships with vendors. Steve is the proud father of three children, two sons and one daughter. Steve's son was soon to start college at an Ivy League school. Although immensely proud, Steve was worried about making tuition payments as well as providing for the rest of his family. After his son's freshman year, things began to get really tight. Not wanting his son to know that the family was hurting financially, he decided to talk to a vendor who was interested in doing business with the company. After accepting the first kickback, the second was easier. Soon Steve was able to pay for his son's tuition and more. He began buying expensive jewelry for his wife and taking extravagant trips. Because Mary was a personal friend, she inquired where the money was coming from. Steve told Mary that his wife had received an inheritance from an aunt. Because Mary trusted him, she believed his story. She did not become suspicious until one day she tried to contact a vendor directly. Steve would not allow her to do so and insisted that she talk to the vendor through him. Soon Mary discovered that Steve had taken a substantial amount of money and had taken advantage of their trusting relationship. How could this fraud have been prevented?

Case 9

Robert was the chief teller in a large New York bank. Over a period of three years, he embezzled $1.5 million. He took the money by manipulating dormant accounts. Unfortunately, Robert was both responsible for handling dormant accounts and for dealing with complaints from customers. When a customer would complain about his account, Robert was always the one to explain the discrepancy. He usually used the excuse that "it's a computer error." What internal control weaknesses allowed this fraud to occur?

Case 10

A controller of a small fruit-packing company in California stole $212,000 from the company. When asked why, he said, "Nobody at the company (especially the owners) ever talked to me. They treated me unfairly, they talked down to me, and they were rude to me. They deserve everything they got." What could the company have done to prevent this fraud?

Case 11

Jorge recently graduated with his MBA from a prestigious Ivy League school. Lacking external financial support, Jorge was forced to finance his MBA with a significant amount of student debt. Unfortunately, he also developed a love of eating out and golfing that exacerbated his debt problem, as he financed his expensive outings with credit cards. Jorge was not as successful as he had hoped and secured a job that paid substantially less than what he had anticipated making when he took out his student loans. After graduation, his monthly loan payments were a significant financial burden. Further, soon after starting work, Jorge's mother died, and Jorge became clinically depressed which engendered even more poor financial management. About this time, Jorge also started drinking. Is Jorge at a higher risk for fraud than a normal person? Why? How might an employee assistance program help Jorge?

Case 12

MegaGlobular is a large, private international corporation that has been experiencing problems with fraud. Management has heard of the success other companies have had with whistle-blowing programs mandated by the Sarbanes-Oxley Act and decides to implement a formal whistle-blower system and other fraud prevention programs. In every office, they assign an employee to be the fraud liaison, usually someone in middle management. They hang signs in all break rooms alerting employees about the liaisons. The signs instruct employees to call the liaisons and report any observed fraud. After a year, MegaGlobular realized it was having minimal success with its whistle-blowing program, no one had called liaisons, and the number of frauds was unchanged. What went wrong? How could MegaGlobular change its program to get a better response?

Case 13

Your friend Mark Ambrose runs a small convenience store. He recently fired an employee who had repeatedly stolen merchandise when closing the store alone. Mark is now looking for a replacement and asks for your advice on how he can make sure he hires someone that will be honest. Given the small scale of his operation, he needs someone he can trust, as they will often be working alone with the merchandise and the cash register. What would you advise Mark to do?

Case 14

You are the owner of a privately owned, moderate-sized company. The business was founded over 20 years ago and has experienced impressive growth and profitability. The only frustrating thing, however, is that you know the company's profits would be significantly higher if you could rid it of its problems with fraud. Your accountants estimate that the company has lost approximately 7 percent of its earnings to fraud over the past five years. The company has adequate controls in place, and you try to ensure that people don't override them. Since you are the owner, however, you often bypass some controls. You know that you aren't out to rob the company, so you believe that the controls aren't applicable to you. You try to keep a close eye on most aspects of the business, but with about 500 employees, it's difficult to know about everything that is going on. Employees have been caught in fraudulent activities in the past, but you have never bothered prosecuting them. You wish to avoid the negative publicity that would result, and you see no valid reason to publicly humiliate former employees—their shame won't bring back the money they've stolen. Questions: What aspects of the company can you change in order to reduce the amount of fraud that is occurring? Use the five factors described in the chapter relating to creating a culture of honesty, openness, and assistance to explain your answer.

CASE STUDIES

Case Study 1

May 13, 1988, a Friday incidentally, will be remembered by a major Chicago bank. Embezzlers nearly escaped with $69 million! Arnand Moore, who was released after serving four years of his 11-year sentence for a $180,000 fraud, decided it was time to put his fingers in something a little bigger and better. He instigated a $68.7 million fraud plan. Naming himself as "Chairman," he assembled Herschel Bailey, Otis Wilson, Neal Jackson, Leonard Strickland, and Ronald Carson to complete the formation of his "Board." Most importantly, the "Board" was able to convince an employee of the Chicago bank to provide their "in." The caper required one month of planning in a small hotel in Chicago and took all of 64 minutes to complete.

The bank employee had worked for the Chicago bank for eight years, and he was employed in the bank's wire-transfer section, which dispatches multimillion-dollar sums around the world via computers and phone lines. Some of the bank's largest customers send funds from their accounts directly to creditors and suppliers. For electronic transfers, most banks require that a bank employee call back another executive at the customer's offices to reconfirm the order, using various code numbers. All such calls are automatically taped. The crooked employee participated in these deposits and confirmations, and he had access to all the code numbers and names of appropriate executives with whom to communicate.

The "Board's" targets were Merrill Lynch, United Airlines, and Brown-Forman Distillers. A few members of the gang set up phony bank accounts in Vienna under the false names of "Lord Investments," "Walter Newman," and "GTL Industries." At 8:30 a.m., a gang member posing as a Merrill Lynch executive called the bank to arrange a transfer of $24 million to the account of "Lord Investments," and was assisted by one of the crooked employee's unsuspecting coworkers. In accordance with the bank's practice of confirming the transfers with a second executive of the company, the employee stepped in and called another supposed "Merrill Lynch" executive who was actually Bailey, his partner in crime. Bailey's unfaltering, convincing voice was recorded automatically on the tape machine, and the crooked employee wired the funds to Vienna via the New York City bank. The same procedure followed at 9:02 and 9:34 a.m. with phony calls on behalf of United Airlines and Brown-Forman. The funds were initially sent to Citibank and Chase Manhattan Bank, respectively.

On Monday, May 16, the plot was uncovered. The "Chairman" and his "Board" were discovered due to no effort on the part of the Chicago bank nor any investigative authority. Although bank leaders do not like to admit just how close the culprits came to "getting away with it," investigators were amazed at how far the scheme proceeded before being exposed. Had the men been a little less greedy, say possibly $40 million, or if they had chosen accounts that were a little less active, they may have been touring the world to this day! The plot was discovered because the transfers overdrew the balances in two of the accounts, and when the companies were contacted to explain the NSF transactions, they knew nothing about the transfers.

Questions

1. How could this fraud have been prevented? Why is this a difficult fraud to prevent?

Case Study 2

Code of Ethics ABC Enterprises has developed the following code of ethics:

Corporate Governance Code of Ethics for Financial Professionals

This Code of Ethics for Financial Professionals (the "Code of Ethics") applies to the Chief Executive Officer, Chief Financial Officer and all professionals worldwide serving in a finance, accounting, treasury, tax or investor relations role at ABC Enterprises, Inc. ("ABC"). ABC expects all of its employees to act in accordance with the highest standards of personal and professional integrity in all aspects of their activities. ABC therefore has existing Codes of Ethics and Business Conduct applicable to all directors, officers and employees of ABC. In addition to the Codes of Ethics and Business Conduct, the CEO, CFO and all other financial professionals are subject to the following additional specific policies: As the Chief Executive Officer, Chief Financial Officer, or other financial professional, I agree to:

- **a.** *Engage in and promote honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;*
- **b.** *Avoid conflicts of interest and to disclose to the General Counsel any material transaction or relationship that reasonably could be expected to give rise to such a conflict;*
- **c.** *Take all reasonable measures to protect the confidentiality of non-public information about ABC or its subsidiaries and their customers obtained or created in connection with my activities and to prevent the unauthorized disclosure of such information unless required by applicable law or regulation or legal or regulatory process;*
- **d.** *Produce full, fair, accurate, timely, and understandable disclosure in reports and documents that ABC or its subsidiaries files with, or submits to, the Securities and Exchange Commission and other regulators and in other public communications made by ABC or its subsidiaries;*
- **e.** *Comply in all material respects with applicable governmental laws, rules and regulations, as well as the rules and regulations of the New York Stock Exchange and other appropriate private and public regulatory agencies; and*
- **f.** *Promptly report any possible violation of this Code of Ethics to the General Counsel or any of the parties or through any of the channels described in ABC's Whistleblower Policy.*

I understand that I am prohibited from directly or indirectly taking any action to fraudulently influence, coerce, manipulate or mislead ABC or its subsidiaries' independent public auditors for the purpose of rendering the financial statements of ABC or its subsidiaries misleading.

I understand that I will be held accountable for my adherence to this Code of Ethics. My failure to observe the terms of this Code of Ethics may result in disciplinary action, including termination of employment. Violations of this Code of Ethics may also constitute violations of law and may result in civil and criminal penalties against me, my supervisors and/or ABC.

Any questions regarding the best course of action on a particular situation should be directed to the General Counsel. Please be aware that ABC's Whistleblower Policy provides the option to remain anonymous in reporting any possible violation of the Code of Ethics.

Questions

1. ABC Enterprises has created multiple codes of conduct applicable to different groups of employees. Why wouldn't they create just one code of conduct, applicable to everyone in the company?
2. Who, specifically, has agreed to follow the "Code of Ethics for Financial Professionals"?
3. How is ABC helping to prevent white-collar crime within its company by defining and clarifying appropriate and inappropriate behavior in its codes of conduct?

INTERNET ASSIGNMENTS

1. As mentioned in the chapter, the Committee of Sponsoring Organizations produced several reports on internal control. One of these relates to internal controls over financial reporting for smaller companies.

Visit the Web site at red hat code of business conduct and ethics www.coso.org and read how the commission defines "smaller companies." What is their definition?

2. Go to www.insurancefraud.org and read the information about insurance fraud for consumers.

Insurance fraud is a problem that has become increasingly costly for the insurance industry. The Coalition

Against Insurance Fraud estimates that insurance losses are at least $90 billion per year or $950 per family. Besides the dollar costs of insurance fraud, what are the other ways discussed in the article that Americans are hurt by insurance fraud?

DEBATES

1. You work for a small manufacturing firm, where it is clearly too expensive to have proper segregation of duties. Because of this lack of control, management knows that opportunities exist to perpetrate fraud within the company. Management is particularly concerned with possible collusion between purchasing agents and vendors because of the relatively small size of the company and the fact that a single purchasing agent is often solely responsible for a vendor's account. Management knows now that a lot of money can be saved by proactively preventing fraud and not just acting on a reactionary or crisis basis. They have started to establish an open-door policy where all employees are encouraged to talk about pressures and opportunities faced while on the job. Management also wants to establish a hotline where employees can report suspicious activity.

   a. Is an employee hotline necessary?
   b. Is this sort of whistle-blowing ethical?
   c. What can management do as they establish this hotline to encourage employees to actually use it?

2. During the past year, your company has discovered three major frauds. The first was a $3.9 million theft of inventory that had been going on for six years. The second was a $2.8 million kickback scheme involving the most senior purchasing agent. She had been allowing certain customers to overcharge for products in return for personal payments and other financial favors. The third was an overstatement of receivables and inventories by a subsidiary manager to enhance reported earnings. Without the overstatement, his unit's profit would have fallen far short of budget. The amount of overstatement has yet to be determined. All three of these frauds have been reported in the financial newspapers and have been embarrassing to the company.

   In response to these incidents, the board of directors has demanded that management take "positive steps to eliminate future fraud occurrences." In their words, they are "sick and tired of significant hits to the bottom line and negative exposure in the press." The responsibility to develop a program to eradicate fraud has fallen on your shoulders. You are to outline a comprehensive plan to prevent future frauds. In devising your strategy, outline the roles the following groups will play in preventing fraud:

   - Top Management
   - Middle Management
   - Internal Audit
   - Corporate Security
   - Audit Committee
   - Legal Counsel

   Why are each of the groups above reluctant to take the responsibility for detecting and preventing fraud? Who should be responsible? Debate the issues.

END NOTES

1. Albrecht, C., 2007, "A Comment on Koerber and Neck's (2007) 'Religion in the Workplace: Implications for Financial Fraud and Organizational Decision Making,'" *Journal of Management, Spirituality, and Religion*, 4:1.
2. Job Hunting, http://andreakay.com/articles/job-hunting/lying-on-resumes/, accessed June 13, 2007.
3. www.abcnews.go.com/GMA/story?id=1643683, accessed June 13, 2007.
4. www.pnafoundation.org/Training/ColumsBy EdMiller/Power.htm, accessed May 25, 2004.
5. E. Thomas Garman, Irene E. Leech, and John E. Grable, 1996, "The Negative Impact of Employee Poor Personal Financial Behaviors on Employers," *Financial Counseling and Planning*, 7.
6. http://stage.theiia.org/theiia/about-the-profession/internal-audit-faqs/?i=3087, accessed June 14, 2007.
7. Committee of Sponsoring Organizations, 1992, *Internal Control—Integrated Framework*, Treadway Commission.
8. www.deloitte.com/dtt/alert/0,2296,sid%253D5628%2526cid%253D42825,00.html, accessed May 26, 2004.
9. www.toshiba.co.jp/csr/en/compliance/index.htm, accessed June 14, 2007.