FRAUD-RELATED
INTERNAL CONTROLS

(No. 01-5409)
II. THE COSO INTERNAL CONTROL MODEL

This chapter analyzes the model that the Committee of Sponsoring Organizations (COSO) developed to categorize internal controls, relative to the following:

- Control environment
- Control activities
- Risk assessment
- Information and communication
- Monitoring performance

Control Environment

An effective control environment consists of many factors, including:

- Commitment to integrity and ethical values
- Management’s philosophy and operating style
- Organizational structure
- The Audit Committee of the Board of Directors
- Methods of assigning authority and responsibility
- Human resources policies and practices
- External influences

Commitment to Integrity and Ethical Values

It is important for management to create an organizational culture that stresses integrity and ethical values. Companies can do this by endorsing integrity as a basic principle of the company, as well as by personally and actively teaching and practicing it. For example, top management should make it clear that honest reports are more important than favorable reports. Management should not assume that everyone accepts honesty, and it should consistently reward and encourage honesty, giving verbal labels to both honest and dishonest behavior. If companies simply punish dishonesty or reward honesty without providing a label or explaining the principle—or if the standard of honesty is applied inconsistently—employees will likely be inconsistent in their moral behavior.

Management should develop clear policies that explicitly describe honest and dishonest behaviors. These policies should focus on issues that are uncertain or unclear, such as conflicts of interest and the acceptance of gifts. For example, most purchasing agents would agree that accepting a $5,000 bribe from a supplier is dishonest, but a weekend vacation at a hunting cabin is not as clear-cut of a decision. Dishonesty, to a large degree, results from rationalizing such situations.
The COSO Internal Control Model

All dishonest acts should be thoroughly investigated, and those found guilty should be dismissed. Enough dishonest employees should be prosecuted so that all employees know that dishonesty will be punished, not tolerated.

Management’s Philosophy and Operating Style
The more responsible management’s philosophy and operating style, the more likely it is that employees will behave responsibly in working to achieve the organization’s objectives. If management shows little concern for internal controls, employees are less diligent and effective in achieving specific control objectives.

Management’s philosophy and operating style can be assessed by answering questions such as the following:
• Does management take undue business risks to achieve its objectives, or does it assess potential risks and rewards prior to acting?
• Does management attempt to manipulate performance measures (e.g., net income) so that its performance can be seen in a more favorable light?
• Does management pressure employees to achieve results regardless of the methods, or does it demand ethical behavior? In other words, does it believe the end justifies the means?

Organizational Structure
A company’s organizational structure defines its lines of authority and responsibility, and provides the overall framework for planning, directing, and controlling its operations. Important aspects of organizational structure include:
• The centralization or decentralization of authority.
• The assignment of responsibility for specific tasks.
• The way responsibility allocation affects management’s information requirements.
• The organization of the accounting and information system functions.

An overly complex or unclear organizational structure may indicate more serious problems. ESM, a brokerage company dealing in government securities, used a multi-layered organizational structure to hide a $300 million fraud. Company officers funneled cash to themselves, hiding it in their financial statements by reporting a fictitious receivable from a related company.

In today’s business world, drastic changes are occurring in management practices and in the organization of companies. Hierarchical organizational structures, with many layers of management who supervise and control the work of those under them, are disappearing. They are being replaced with flat organizations that have self-directed work teams composed of employees formerly assigned to separate and segregated departments. Team members are empowered to make decisions and no longer have to
seek multiple layers of approvals to complete their work. There is an emphasis on continuous improvement rather than the periodic reviews and appraisals characteristic of earlier evaluators. These changes have an enormous impact on a company’s organizational structure and on the nature and type of controls used in organizations.

**The Audit Committee of the Board of Directors**

All corporations listed on the New York Stock Exchange (NYSE) must have an audit committee composed entirely of outside (non-employee) directors. The audit committee is responsible for overseeing the corporation’s internal control structure, its financial reporting process, and its compliance with related laws, regulations, and standards. The committee works closely with the corporation’s external and internal auditors. One of the committee’s responsibilities is to provide an independent review of the actions of corporate managers on behalf of company shareholders. This review serves as a check on management integrity and increases the confidence of the investing public in the propriety of financial reporting.

**Methods of Assigning Authority and Responsibility**

Management should assign responsibility for specific business objectives to specific departments and individuals and then hold them accountable for achieving those objectives. Authority and responsibility may be assigned through formal job descriptions, employee training and operating plans, schedules, and budgets. Of particular importance is a formal company code of conduct addressing such matters as standards of ethical behavior, acceptable business practices, regulatory requirements, and conflicts of interest.

A written policy and procedures manual is an important tool for assigning authority and responsibility, and spelling out management policies with respect to handling specific transactions. In addition, it documents the systems and procedures employed to process those transactions and includes the organization’s chart of accounts as well as sample copies of forms and documents. The manual is a helpful on-the-job reference for employees and a useful tool in training new employees.

**Human Resources Policies and Practices**

Some computer consultants claim that the most effective method of obtaining adequate internal control is to rely on the integrity of company employees. However, research by the Association of Certified Fraud Examiners, as reflected in its 2010 *Report to the Nations on Occupational Fraud and Abuse*, shows that most fraud is committed by employees and mid-level managers. Thus, employees can be both the greatest control strength and the greatest weakness in a business. Organizations must take steps to increase employee integrity and reduce the likelihood that employees will commit fraud. Policies and
practices dealing with hiring, training, evaluating, compensating, and promoting employees affect an organization’s ability to minimize threats, risks, and exposures.

Policies with respect to working conditions, compensation, job incentives, and career advancement can be a powerful force in encouraging efficiency and loyal service. Additional control policies are needed for employees with access to cash or other property. These employees should be required to take an annual vacation, and during this time, other staff members should perform their jobs. Many employee frauds are discovered when the perpetrator is suddenly forced by illness or accident to take time off. Periodic rotation of duties among key employees can achieve the same results. Of course, the very existence of such policies deters fraud and enhances internal control. Finally, fidelity bond insurance coverage of key employees protects companies against losses arising from deliberate acts of fraud by bonded employees.

Many fraud schemes, such as lapping and kiting, require the ongoing attention of the perpetrator. If mandatory vacations were coupled with a temporary rotation of duties, these ongoing fraud schemes would fall apart. For example, when federal investigators raided an illegal gambling establishment, they found that Roswell Steffen, who earned $11,000 per year, was betting up to $30,000 a day at the racetrack. Investigators at Union Dime Savings Bank discovered he had embezzled and gambled away $1.5 million of their money over a three-year period. A compulsive gambler, Steffen started out by borrowing $5,000 to place a bet on a “sure thing” that did not pan out. He embezzled ever-increasing amounts trying to win back the original money he had “borrowed.” Steffen committed his fraud by transferring money from inactive accounts to his own account. If the owner of an inactive account complained, Steffen, who as the chief teller had the power to resolve these types of problems, replaced the money by taking it from some other inactive account. After being caught and asked how the fraud could have been prevented, he said the bank could have coupled a two-week vacation period with several weeks of rotation to another job function. That would have made his embezzlement, which required his physical presence at the bank and his constant attention, almost impossible to cover up.

Employees should be informed of the consequences of using illegal copies of software, and the company should institute controls to see that illegal copies are not in use. Software license management, a fast-growing area of information technology management, helps companies make sure they comply with all their software licenses. Of key concern is making sure there are enough licenses to meet user demands and that the number of users does not exceed the number of licenses. This protects the company from software piracy lawsuits and can save the company money by ensuring that it does not pay for more licenses than it actually needs.
**Hiring**

Employees should be hired and promoted based on how well they meet written job requirements. Resumes, reference letters, and background checks are important means of evaluating the qualifications of job applicants. The importance of thorough background checks is underscored by the case of Philip Crosby Associates (PCA), a consulting and training firm. PCA undertook an exhaustive search to select a financial director, and hired John Nelson, an MBA and CPA with a glowing reference from his former employer. In reality, the CPA and reference were phony. Nelson was really Robert W. Liszewski who had recently served an 18-month jail sentence for embezzling $400,000 from an Indiana bank. By the time PCA discovered this, Liszewski had embezzled $960,000 using wire transfers to a dummy corporation supported by forged signatures on contracts and authorization documents.

Some people, intent on breaking into systems, will pose as temporary employees because they are given access to the information system, but are not subjected to normal hiring practices such as background checks. Once able to legitimately access the system, they are able to use any number of techniques to commit fraud or sabotage it. Other people take jobs as janitors to afford them after-hours access to the premises and hopefully get unauthorized access to company resources or information, or to log into the computer system. This technique was popularized by a story in *2600 Magazine* (a hacker quarterly) that explained how to get a job as a janitor in order to crack into a company's computers. For this reason, all company personnel, including cleaning crews and temporary employees, should be subject to all hiring and firing policies.

**Firing**

A company should be very careful when firing employees. Dismissed employees should be removed from sensitive jobs immediately and denied access to the computer system to prevent sabotage or copying of confidential data before they leave. One employee, after learning he had been terminated, lit a butane lighter under a smoke detector located just outside the computer room, thus setting off a sprinkler system that ruined most of the computer hardware.

**Handling Disgruntled Employees**

Many employees who commit fraud are seeking revenge or “justice” for some wrong they perceive has been done to them. Hence, companies should have procedures for identifying these individuals and either helping them resolve their feelings, or removing them from jobs with system access. One way to avoid having disgruntled employees and to maintain high company morale is to provide grievance channels and employee counseling. Employees need someone outside the normal chain of command to talk with about their grievances and problems. Having someone who will listen to them and help them resolve their problems can significantly decrease the number of dissatisfied employees. This is often not
easy to accomplish since most employees fear that airing their feelings could have negative consequences for their careers.

**Employee Training**

Training programs should familiarize new employees with their responsibilities, as well as with organizational policies and procedures. Many top executives believe that employee training and education is the most important element of any security program. Fraud is much less likely to occur in an environment where employees believe that security is everyone’s business. An ideal corporate culture for fraud deterrence exists when employees are proud of their company and protective of its assets. They believe in their responsibility to report fraud because what harms the company harms them. But this culture does not just happen; it has to be created, taught, and practiced.

To develop this type of culture, a company should educate and train employees in the following areas:

- **Security measures.** Employees should be well schooled in security measures, taught why the measures are important, and motivated to take them very seriously. Security should be monitored and enforced as a way of reinforcing this training.

- **Telephone disclosures.** Employees should be taught to not offer confidential information over the telephone without knowing who is calling. Employees can be taught tactics such as dialing the caller back and verifying his identity by asking penetrating and specific questions that only the caller would be able to answer.

- **Fraud awareness.** Employees should be made aware of fraud, its prevalence, and its dangers. They should be taught why people commit fraud, and how to deter and detect it.

- **Ethical considerations.** The company should promote its ethical standards in its practices and through company literature, such as employee handouts. Acceptable and unacceptable behavior should be defined so that employees are aware of a company’s ethical position should a problem arise. Many business practices fall into a gray area between right and wrong, a problem particularly prevalent throughout the computer industry. For example, many professionals see nothing wrong with utilizing corporate computer resources for personal use, or gaining unauthorized access to another company’s databases and browsing through them. One programmer, when arrested for unauthorized browsing, was shocked that he was prosecuted for his “crime”; he felt his activities were a common industry practice.

- **Punishment for unethical behavior.** Employees should be informed of the consequences of unethical behavior (e.g., reprimands, dismissal, or prosecution). This information should be disseminated, not as a threat, but as the consequence of choosing to act unethically. For example, employees should be informed that using a computer to steal or commit fraud is a federal crime, and anyone so doing faces immediate dismissal and/or prosecution. Likewise, the company should display notices of program and data ownership, and inform employees of the penalties of misuse.
Educating employees about security issues, fraud awareness, ethical considerations, and the consequences of choosing to act unethically can make a tremendous difference. Such education can be accomplished through informal discussions and formal meetings, periodic departmental memos, written guidelines and codes of professional ethics, circulating reports of securities violations and their consequences, and security and fraud training programs.

Confidentiality Agreements
All employees, vendors, and contractors should be required to sign and abide by confidentiality agreements.

Prosecute and Incarcerate Fraud Perpetrators
Most fraud cases go unreported and are not prosecuted for several reasons. First, many cases of computer fraud are as yet undetected. Second, companies are reluctant to report computer crimes because a highly visible computer fraud constitutes a public relations disaster. Fraud also reveals the vulnerability of a company’s system, possibly attracting more acts of fraud. One study found that less than 29 percent of computer abuses were reported to law enforcement officials. Unreported fraud creates a false sense of security; people think systems are more secure than they really are. Third, law enforcement officials and the courts are so busy with violent crimes that they have little time for fraud cases where no physical harm is present. All too often, prosecuting attorneys treat teen hacking and cracking as childish pranks and let the perpetrators plea bargain down to a misdemeanor.

A fourth reason fraud goes unreported is that it is difficult, costly, and time-consuming to investigate. Successfully prosecuting computer fraud cases is difficult. Until 1986, there were no laws that dealt specifically with computer crimes. As a result, law enforcement officials had to prosecute using laws written for other purposes. This problem was partially resolved when Congress passed the Computer Fraud and Abuse Act of 1986, a law covering computers used by the federal government, financial institutions, and certain medical organizations. It also covers computers used in interstate or foreign commerce. The law makes it illegal to knowingly gain access to computers with intent to defraud. Trafficking in computer access passwords is also prohibited. The crime is a felony if more than $1,000 worth of software is damaged, or if money, goods, or services are stolen. The penalties are severe: one to five years of imprisonment for the first offense, 10 years for the second, and 20 years for three or more offenses. Fines up to $250,000, or twice the value of the stolen data, are possible. Although the law has resulted in increased prosecutions, many people declare it to be vague and unclear—an easy target for defense attorneys. Federal law is supplemented with computer fraud statutes in all 50 states.

A fifth reason for unreported fraud is that many law enforcement officials, lawyers, and judges lack the computer skills needed to properly investigate, prosecute, and evaluate computer crimes. Increased
training, a time-consuming and costly proposition, is necessary in order for officials to understand and detect computer fraud.

Finally, when fraud cases are prosecuted and a conviction is obtained, the sentences received are often very “light.” For example, Judge John Lord, when sentencing convicted white-collar criminals, stated that the perpetrators were God-fearing, highly civic-minded men, who had spent their lifetimes in sincere and honest dedication and service to their families, churches, country, and communities. He said he could never send them to jail. One investigator noted that the average sentence for a fraud perpetrator was one year in jail for every $10 million stolen.

One of the most famous cases involving a light sentence involved C. Arnoldt Smith, former owner of the San Diego Padres baseball team, a man who was named Mr. San Diego of the Century. Smith was very involved in the local community and made large political contributions. When investigations showed that he had stolen $200 million from his bank, he pleaded *nolo contendere* (no contest). Smith, 71 at the time, was given a sentence of four years of probation and a fine of $30,000. The fine was to be paid at the rate of $100 a month for 25 years, with no computed interest. The embezzled money was never recovered.

**External Influences**

External influences affecting an organization’s control environment include requirements imposed by stock exchanges, by the Financial Accounting Standards Board (FASB), by the Securities and Exchange Commission (SEC), and by regulatory agency requirements, such as those for banks, utilities, and insurance companies. Examples include enforcement of the internal control provisions of the Foreign Corrupt Practices Act by the SEC and audits of financial institutions by the Federal Deposit Insurance Corporation (FDIC).

**Control Activities**

The second component of COSO’s internal control model is *control activities*. Control activities are policies and rules that provide reasonable assurance that management’s control objectives will be achieved.

Generally, control procedures fall into one of five categories:

- Proper authorization of transactions and activities
- Segregation of duties
- Design and use of adequate documents and records
- Adequate safeguards over access to and use of assets and records
- Independent checks on performance
Violation of specific control activities, combined with control environment factors, resulted in a fraud at a school district in the Midwest. The director of finance for the school district, which had 42 separate schools, hired a CPA firm to audit the school district books. The audit was accompanied by a report showing that the district’s system had a number of serious internal control deficiencies. The director, a former auditor, went to work to improve the control system. The district (1) selected a new software package that all sites would use, (2) standardized accounting and bookkeeping procedures, (3) instituted consistent purchase order procedures, (4) implemented a separation of duties, and (5) created a control system for student vending machine cash and inventory.

As the changes were being made, the director noted that book collection fees for the middle school were low, and asked the district’s internal auditor to investigate. The auditor contacted the middle school secretary responsible for making daily deposits of all student fees and writing checks to the central office for book fees. The secretary said the low amount was due to the increase in the number of fees waived by the principal for students who qualified for free or reduced lunches.

The principal denied that he was waiving the fees. The principal, the auditor, and the director examined the fee cards for each child. Their investigation showed that the daily deposits into the activity checking account did not agree with the dates stamped “paid” on the student fee cards. A thorough search of the premises revealed no uncashed checks. So where did the money go, and how did the secretary manage to take it when most of the fees were paid with checks written to the school?

The auditor finally discovered that the secretary was also in charge of the faculty welfare and vending machine receipts fund. The district was not responsible for the fund, so it was neither audited nor examined. Nor was the fund subject to the newly implemented system of internal controls. Deposits to the welfare fund consisted of checks from the faculty and cash from the vending machines.

An examination of the available records revealed how the $20,000 fraud took place. The secretary stole all cash received from the vending machines. She wrote and recorded checks to vendors. However, on some checks she erased the name of the payee and replaced it with her name. She deposited student fees into the faculty welfare to cover up the stolen funds.

The secretary was immediately discharged due to improper bookkeeping practices. She was bonded, so the district was able to recover all of its missing funds.

As a result, the school district made a number of changes to strengthen control. Internal auditors now examine all funds at the schools. The control of faculty welfare funds was transferred to a faculty member. And since the investigation revealed that the secretary had a prior criminal record, a background check was implemented so that all future hires would be screened.
Proper Authorization of Transactions and Activities

Employees perform tasks and make decisions that affect company assets. Management has neither the time nor resources to supervise each activity or decision. Instead, it establishes policies for employees to follow, empowering them to perform activities and make decisions. Such empowerment, called *authorization*, is an important part of an organization’s control procedures. Authorization is often documented by signing, initialing, or entering an authorization code on a transaction document or record. Computer systems are now capable of recording a digital signature (or digital fingerprint), which is a means of signing a document using a piece of data that can’t be forged.

Employees who process transactions should verify the presence of the appropriate authorization(s). Auditors review transactions to verify proper authorization, since their absence indicates that a control problem may exist.

Certain activities or transactions may be of such consequence that management grants specific authorization for them to occur. For example, management review and approval is often required for sales in excess of $20,000, capital expenditures in excess of $10,000, or uncollectible write-offs in excess of $5,000. In contrast, management can authorize employees to handle routine transactions without special approval, a procedure known as *general authorization*. Management should have written policies on both specific and general authorization for all types of transactions. Table 2.1 shows some examples of authorization functions.