**­­Chapter Six – Internal Controls and Cash**

We all are aware of theft and fraud. They affect us in several ways: We lock doors, chain bikes, review sales receipts, and acquire alarm systems. A company also takes actions to safeguard, control, and manage what it owns. Experience tells us that small companies are most vulnerable, usually due to weak internal controls. It is management's responsibility to set up policies and procedures to safeguard a company's assets, especially cash. To do so, management *and* employees must understand and apply principles of internal control. This chapter describes these principles and how to apply them. It focuses special attention on cash because it is easily transferable and is often at high risk of loss.

**INTERNAL CONTROL**

This section describes internal control and its fundamental principles. We also discuss the impact of technology on internal control and the limitations of control procedures.

**Purpose of Internal Control**

Managers (or owners) of small businesses often control the entire operation. These managers usually purchase all assets, hire and manage employees, negotiate all contracts, and sign all checks. They know from personal contact and observation whether the business is actually receiving the assets and services paid for. Most companies, however, cannot maintain this close personal supervision. They must delegate responsibilities and rely on formal procedures rather than personal contact in controlling business activities.

Internal Control System Managers use an internal control system to monitor and control business activities. An **internal control system** consists of the policies and procedures managers use to

* Protect assets.
* Ensure reliable accounting.
* Promote efficient operations.
* Urge adherence to company policies.

A properly designed internal control system is a key part of systems design, analysis, and performance. Managers place a high priority on internal control systems because they can prevent avoidable losses, help managers plan operations, and monitor company and employee performance. Internal controls do not provide guarantees, but they lower the company's risk of loss.

Sarbanes-Oxley Act (SOX) The **Sarbanes-Oxley Act (SOX)** requires the managers and auditors of companies whose stock is traded on an exchange (called *public companies*) to document and certify the system of internal controls. Following are some of the specific requirements:

* Auditors must evaluate internal controls and issue an internal control report.
* Auditors of a client are restricted as to what consulting services they can provide that client.
* The person leading an audit can serve no more than seven years without a two-year break.
* Auditors' work is overseen by the *Public Company Accounting Oversight Board* (PCAOB).
* Harsh penalties exist for violators—sentences up to 25 years in prison with severe fines.

SOX has markedly impacted companies, and the costs of its implementation are high. Importantly, **Section 404** of SOX requires that managers document and assess the effectiveness of all internal control processes that can impact financial reporting. The benefits include greater confidence in accounting systems and their related reports. However, the public continues to debate the costs versus the benefits of SOX as nearly all business activities of these companies are impacted by SOX. Section 404 of SOX requires that managers document and assess their internal controls *and* that auditors provide an opinion on managers' documentation and assessment. Costs of complying with Section 404 for companies is reported to average $4 million (source: Financial Executives Institute).

**Principles of Internal Control**

Internal control policies and procedures vary from company to company according to such factors as the nature of the business and its size. Certain fundamental internal control principles apply to all companies. The **principles of internal control** are to

1. Establish responsibilities.
2. Maintain adequate records.
3. Insure assets and bond key employees.
4. Separate recordkeeping from custody of assets.
5. Divide responsibility for related transactions.
6. Apply technological controls.
7. Perform regular and independent reviews.

**Point: Sarbanes-Oxley Act (SOX)** requires that each annual report contain an *internal control report*, which must: (1) state managers' responsibility for establishing and maintaining adequate internal controls for financial reporting; and (2) assess the effectiveness of those controls.

This section explains these seven principles and describes how internal control procedures minimize the risk of fraud and theft. These procedures also increase the reliability and accuracy of accounting records. A framework for how these seven principles improve the quality of financial reporting is provided by the **Committee of Sponsoring Organizations (COSO)**. Specifically, these principles link to five aspects of internal control: control activities, control environment, risk assessment, monitoring, and communication.

**Establish Responsibilities**

Proper internal control means that responsibility for a task is clearly established and assigned to one person. When a problem occurs in a company where responsibility is not identified, determining who is at fault is difficult. For instance, if two salesclerks share the same cash register and there is a cash shortage, neither clerk can be held accountable. To prevent this problem, one clerk might be given responsibility for handling all cash sales. Alternately, a company can use a register with separate cash drawers for each clerk. Most of us have waited at a retail counter during a shift change while employees swap cash drawers.

**Maintain Adequate Records**

Good recordkeeping is part of an internal control system. It helps protect assets and ensures that employees use prescribed procedures. Reliable records are also a source of information that managers use to monitor company activities. When detailed records of equipment are kept, for instance, items are unlikely to be lost or stolen without detection. Similarly, transactions are less likely to be entered in wrong accounts if a chart of accounts is set up and carefully used. Many preprinted forms and internal documents are also designed for use in a good internal control system. When sales slips are properly designed, for instance, sales personnel can record needed information efficiently with less chance of errors or delays to customers. When sales slips are prenumbered and controlled, each one issued is the responsibility of one salesperson, preventing the salesperson from pocketing cash by making a sale and destroying the sales slip. Computerized point-of-sale systems achieve the same control results.

**Insure Assets and Bond Key Employees**

Good internal control means that assets are adequately insured against casualty and that employees handling large amounts of cash and easily transferable assets are bonded. An employee is *bonded* when a company purchases an insurance policy, or a bond, against losses from theft by that employee. Bonding reduces the risk of loss. It also discourages theft because bonded employees know an independent bonding company will be involved when theft is uncovered and is unlikely to be sympathetic with an employee involved in theft.

**Separate Recordkeeping from Custody of Assets**

A person who controls or has access to an asset must not keep that asset's accounting records. This principle reduces the risk of theft or waste of an asset because the person with control over it knows that another person keeps its records. Also, a recordkeeper who does not have access to the asset has no reason to falsify records. This means that to steal an asset and hide the theft from the records, two or more people must *collude*—or agree in secret to commit the fraud.

**Divide Responsibility for Related Transactions**

Good internal control divides responsibility for a transaction or a series of related transactions between two or more individuals or departments. This is to ensure that the work of one individual acts as a check on the other. This principle, often called *separation of duties*, is not a call for duplication of work. Each employee or department should perform unduplicated effort. Examples of transactions with divided responsibility are placing purchase orders, receiving merchandise, and paying vendors. These tasks should not be given to one individual or department. Assigning responsibility for two or more of these tasks to one party increases mistakes and perhaps fraud. Having an independent person, for example, check incoming goods for quality and quantity encourages more care and attention to detail than having the person who placed the order do the checking. Added protection can result from identifying a third person to approve payment of the invoice. A company can even designate a fourth person with authority to write checks as another protective measure.

A good system of internal controls will have special journals and subsidiary ledgers to maintain separation of duties.

**Apply Technological Controls**

Cash registers, check protectors, time clocks, and personal identification scanners are examples of devices that can improve internal control. Technology often improves the effectiveness of controls. A cash register with a locked-in tape or electronic file makes a record of each cash sale. A check protector perforates the amount of a check into its face and makes it difficult to alter the amount. A time clock registers the exact time an employee both arrives at and departs from the job. Mechanical change and currency counters quickly and accurately count amounts, and personal scanners limit access to only authorized individuals. Each of these and other technological controls are an effective part of many internal control systems.

**Limitations of Internal Control**

All internal control policies and procedures have limitations that usually arise from either (1) the human element or (2) the cost–benefit principle.

Internal control policies and procedures are applied by people. This human element creates several potential limitations that we can categorize as either (1) human error or (2) human fraud. *Human error* can occur from negligence, fatigue, misjudgment, or confusion. *Human fraud* involves intent by people to defeat internal controls, such as *management override*, for personal gain. Fraud also includes collusion to thwart the separation of duties. The human element highlights the importance of establishing an *internal control environment* to convey management's commitment to internal control policies and procedures. Human fraud is driven by the *triple-threat* of fraud:

* **Opportunity**—refers to internal control deficiencies in the workplace.
* **Pressure**—refers to financial, family, society, and other stresses to succeed.
* **Rationalization**—refers to employees justifying fraudulent behavior.

The second major limitation on internal control is the *cost–benefit principle*, which dictates that the costs of internal controls must not exceed their benefits. Analysis of costs and benefits must consider all factors, including the impact on morale. Most companies, for instance, have a legal right to read employees' e-mails, yet companies seldom exercise that right unless they are confronted with evidence of potential harm to the company. The same holds for drug testing, phone tapping, and hidden cameras. The bottom line is that managers must establish internal control policies and procedures with a net benefit to the company.

**Cash Management**

When companies fail, one of the most common causes is their inability to manage cash. Companies must plan both cash receipts and cash payments. The goals of cash management are twofold:

1. Plan cash receipts to meet cash payments when due.
2. Keep a minimum level of cash necessary to operate.

The *treasurer* of the company is responsible for cash management. Effective cash management involves applying the following cash management principles.

* **Encourage collection of receivables.** The more quickly customers and others pay the company, the more quickly that company can use the money. Some companies have cash-only sales policies. Others might offer discounts for payments received early.
* **Delay payment of liabilities.** The more delayed a company is in paying others, the more time it has to use the money. Some companies regularly wait to pay their bills until the last possible day allowed—although, a company must take care not to hurt its credit standing.
* **Keep only necessary levels of assets.** The less money tied up in idle assets, the more money to invest in productive assets. Some companies maintain *just-in-time* inventory; meaning they plan inventory to be available at the same time orders are filled. Others might lease out excess warehouse space or rent equipment instead of buying it.
* **Plan expenditures.** Money should be spent only when it is available. Companies must look at seasonal and business cycles to plan expenditures.
* **Invest excess cash.** Excess cash earns no return and should be invested. Excess cash from seasonal cycles can be placed in a bank account or other short-term investment for income. Excess cash beyond what's needed for regular business should be invested in productive assets like factories and inventories.

Internal control of cash receipts ensures that cash received is properly recorded and deposited. Cash receipts can arise from transactions such as cash sales, collections of customer accounts, receipts of interest earned, bank loans, sales of assets, and owner investments.

**Over-the-Counter Cash Receipts**

For purposes of internal control, over-the-counter cash receipts from sales should be recorded on a cash register at the time of each sale. To help ensure that correct amounts are entered, each register should be located so customers can read the amounts entered. Clerks also should be required to enter each sale before wrapping merchandise and to give the customer a receipt for each sale. The design of each cash register should provide a permanent, locked-in record of each transaction. In many systems, the register is directly linked with computing and accounting services. Less advanced registers simply print a record of each transaction on a paper tape or electronic file locked inside the register.

Proper internal control prescribes that custody over cash should be separate from its recordkeeping. For over-the-counter cash receipts, this separation begins with the cash sale. The clerk who has access to cash in the register should not have access to its locked-in record. At the end of the clerk's work period, the clerk should count the cash in the register, record the amount, and turn over the cash and a record of its amount to the company cashier. The cashier, like the clerk, has access to the cash but should not have access to accounting records (or the register tape or file). A third employee, often a supervisor, compares the record of total register transactions (or the register tape or file) with the cash receipts reported by the cashier. This record is the basis for a journal entry recording over-the-counter cash receipts. The third employee has access to the records for cash but not to the actual cash. The clerk and the cashier have access to cash but not to the accounting records. None of them can make a mistake or divert cash without the difference being revealed—see the following diagram.