

## 4.4: The Need for Internal Control

---

### Learning Objectives

At the end of this section, students should be able to meet the following objectives:

1. Define “internal control.”
2. Explain a company’s need for internal control policies and procedures
3. Describe the effect that a company’s internal control has on the work of the independent auditor.
4. Identify and apply internal control principles to business situations

*Question: In the previous discussions, the role of the independent auditor is described as adding credibility to financial statements. The reported figures, though, are still the responsibility of management. How do a company and its officials make certain that the information displayed in a set of financial statements is fairly presented?*

*Companies like Alphabet (Google) and Bath and Body Works participate in millions of transactions in hundreds geographically distant locations. Working with that amount of data, gathered from around the world, can be a daunting technological challenge. Some organizations are able to accumulate massive quantities of information with few—if any—problems; others seem to be overwhelmed by the task. The reliability of the numbers gathered for reporting purposes impacts the amount and type of testing that the independent auditor considers necessary. How do companies make certain that their own information is free of material misstatements?*

Answer: The human body is made up of numerous systems that perform specific tasks, such as the breathing of air, the circulation of blood, and the digestion of food. Organizations operate in much the same manner. Systems are designed and set in place by management to carry out essential functions, such as paying employees, collecting cash from customers, managing inventory levels, and monitoring receivable balances. Within each system, individuals are charged with performing specific tasks, often in a preordained sequence. For example, a cash payment received electronically from a customer should be handled in a set way every time that it occurs to ensure that it is properly recorded and protected from theft.

To be efficient and effective, these systems must be carefully designed and maintained. They need to keep company assets secure at a minimum cost. In addition, appropriate record keeping is a required aspect of virtually every system. Thus, employees are properly paid when their salary comes due, but also adequate documentation is maintained of the amounts distributed. The entire function is performed according to company guidelines and a record is maintained.

Well-designed systems generate information that poses a reduced threat of material misstatements. However, simply having systems in place—even if they are properly engineered and constructed—is not sufficient to guarantee both the effectiveness of the required actions and the reliability of the collected data. Thus, extra procedures are built into every system by management to help ensure that every operation is performed as intended and the resulting financial data are reliable. All the redundancies added to a system to make certain that it functions properly are known collectively as **internal control**. For example, a rule requiring two designated employees to sign any check for over \$5,000 (or some other predetermined amount) is part of a company’s internal control. There is no inherent necessity for having a second signature; it is an added safeguard included solely to minimize the chance of theft or error. All actions like this comprise a company’s internal control.

Internal control policies and procedures can be found throughout the various systems of every company.

- One person calculates payroll amounts and a second verifies the amounts.
- One person requests the purchase of an asset and a second authorizes the request.

Internal control is made up of all the procedures that are performed purely to help make certain that each system operates as intended. Systems cannot be considered well designed without the inclusion of adequate internal control. Management is responsible for the development of effective systems but also for all the internal control rules and requirements to ensure that these systems accomplish their stated objectives.

*Question: If a company creates and then maintains good operating systems with appropriate internal control, the financial information that is produced is less likely to contain material misstatements. In performing an audit, is the work of the independent*

*CPA affected by the company's internal control? Does the quality of internal control policies and procedures impact the amount and type of audit testing?*

Answer: As a preliminary step in an audit examination, the CPA gains an understanding of the internal control procedures included within each of these systems that relate to reported financial accounts and balances<sup>1</sup>. The auditor then makes an evaluation of the effectiveness of those policies and procedures. In cases where internal control is both well designed and appears to be functioning as intended, a reduction is possible in the amount of audit testing that is needed. The likelihood of a material misstatement is reduced by the company's own internal control.

To illustrate, assume that a company claims to hold accounts receivable totaling \$12.7 million. The auditor plans to confirm one hundred of the individual balances directly with the customers to substantiate the separate amounts listed in the accounting records. A letter will be written to each of these individuals asking them whether the specified balance is correct. A stamped return envelope will be included.

Although effective, this confirmation process is slow and expensive. During the year, the reporting company applied several internal control procedures within those systems that maintain the receivables balances. These controls are evaluated by the independent CPA and judged to be excellent. As a result, the auditor might opt to confirm only thirty or forty individual accounts rather than the one hundred that had originally been determined. Because of the quality of internal control in the receivable area, the risk of a material misstatement is already low. Less audit testing is necessary.

Thus, at the beginning of an independent audit, the design of the reporting company's internal control and the effectiveness of its procedures are assessed. Only then does the auditor start to seek sufficient evidence to substantiate that each account balance is presented fairly because no material misstatements are included according to U.S. GAAP.

*Question: Besides having fairly presented financial statements, what other reasons do companies have to implement a system of internal control? How big is the problem of fraud in business?*

<https://youtu.be/Tb6QX9Yy1GM>

Internal controls are designed to reduce the opportunity for fraud as shown in the video clip above.

*Question: What principles do companies use to help to determine an appropriate system of internal control to combat fraud and prevent misstated financial statements?*

In 1992 the Committee of Sponsoring Organizations (COSO), first released its Internal Control-Integrated Framework and an updated version in 2013.

COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

The National Commission was sponsored jointly by five major professional associations headquartered in the United States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the National Association of Accountants (now the Institute of Management Accountants [IMA]). Wholly independent of each of the sponsoring organizations, the Commission included representatives from industry, public accounting, investment firms, and the New York Stock Exchange.

COSO's standards have achieved broad acceptance around the world as principles that lead to a quality system of internal control. In the executive summary of COSO's updated framework the following are given as Components of Internal Control. Each of them is interrelated with the others.

### **Control Environment**

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

### **Risk Assessment**

Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.

A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

### **Control Activities**

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

### **Information and Communication**

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.

### **Monitoring Activities**

Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

Internal Control — Integrated Framework • © 2013 Committee of Sponsoring Organizations of the Treadway Commission (COSO).

*Question: What do these principles of internal control look like in practice for employees?*

Chances are very high that either at work or in your interactions with businesses you have encountered internal controls – perhaps without realizing it. Let's consider an example and how it illustrates the internal control. Let's say you are checking out or returning an item at a store. Once in a while, the person helping you has to call over a manager or assistant manager to put in a code or use their key to complete the transaction. So what you just observed is that the store did a risk assessment with regard to the process of returning an item or cancelling an item on the register and they determined that there was an unacceptably high risk that the transaction could be done incorrectly or where the employee by themselves could take assets (cash being the riskiest asset). Once the risk has been identified, then control procedures were put in place. The manager coming to use their code or key is an example of authorization/approval – it has to be someone other than the creator of the transaction to be a good internal control. The cash register or the technology enforces the authorization meaning it keeps the transaction going forward without authorization. If the employee knew the manager's code or had their key then the employee could do two parts of the job and there would not be segregation of duties. How does the employee know to call over the manager for the authorization? While we do not see that part, we can assume that the procedure is part of a training manual reviewed with the employee somewhere. That is the information and communication piece. The technology probably helps with monitoring by keeping track of each time the override is done and by whom. This could be reviewed by the store manager to make sure that the internal control is operating and to see if there are any patterns or anomalies that may indicate a problem with the system. Store cameras could also be used to monitor the

application of this internal control. Of course, if no one looks at the report or the video surveillance then monitoring is not being included in the control system.

**You can probably think of other examples you have seen at work or in business like:**

Expense reports must be authorized by a supervisor or higher (depending on the amount) before an employee is reimbursed – shows authorization and segregation of duties and required documentation

Employee time cards must be approved by a department manager before entered into the payroll system and the employee paid – shows approval and segregation of duties (dept manager does not pay the employee and payroll cannot approve the hours)

Bank and credit card accounts are reconciled to see if the transactions recorded in the accounting records match those recorded by the financial institution. To maintain segregation of duties, this should be done by someone who does not have authorization to pay cash, use the credit card or deposit money.

**Some practical considerations when working with internal control procedures you should remember are:**

Mistakes (unintentional) and fraud (intentional) can both result in misstatements and in missing assets. Both can be hard to detect – mistakes because they are random and fraud because the thief will try to cover it up.

When identifying risks a company faces focus on the assets – nobody steals liabilities – with cash in all its forms (electronic) being the most vulnerable asset because it is the easiest to use if you steal it.

A company's information (including customer data like credit card numbers) is a vulnerable asset and should have multiple internal controls procedures to protect it.

Control activities should be designed to counteract a specific risk identified.

To segregate duties you want to have separate individuals have custody for assets (custody means they have access to potentially steal the asset) and have record keeping for that asset.

Technology safeguards like passwords and access codes are excellent ways to preserve authorization and segregation of duties as long as they are not shared or guessed or hacked.

Referring back to our example of the item being returned and needing authorization by a manager, any internal control procedure can be taken too far. It is not true that if one authorization is good then 2 is better. Just think of the backlog if this kind of transaction required two or three separate approvals – pretty soon the customers would stop coming or employees would ignore the onerous requirement. A good system finds the simplest and most efficient control procedure to combat each risk without piling on extra reviews. It also allows transactions with low risk to continue quickly.

### Check Yourself

An internal control activity is most effective when which of the following is true?

- A. When it was designed after a specific risk was identified during the risk assessment phase.
- B. When the same person takes physical custody of the asset and does the record keeping.
- C. When the activity is done in a weak internal control environment.
- D. When no one is monitoring to make sure that internal control activities are completed.

The correct answer is A. Control activities should address a particular risk of error or fraud. Otherwise the activity may be redundant or not really improve the internal controls. Segregation of duties with regard to physical custody of assets, a foundation of a strong internal control environment and periodic monitoring are all steps that can make internal control activities more effective.

### Key Takeaway

All companies operate by means of numerous systems that carry out designated tasks, such as the collection of cash and the payment of purchases. These systems need to be well designed and operating as intended to reduce the chance of material misstatements. Additional policies and procedures are included at important junctures in the construction of these systems to ensure that they function appropriately. All such safeguards make up the company's internal control system. The independent auditor evaluates the quality of the internal control found in the various systems. If the risk of material misstatement has been reduced as a result of the internal control in a particular system, less audit testing is required.

A properly designed system of internal control employees principles and control procedures that can be applied to a range of business situations.

<sup>1</sup>Some internal controls have nothing to do with a company's financial statement accounts and are not of importance to the work of the independent auditor. For example, a company might establish a review procedure to ensure that only deserving employees receive promotions. This guideline is an important internal control for the operating effectiveness of the company. However, it does not relate to a reported account balance and is not evaluated by the independent auditor.

---

4.4: The Need for Internal Control is shared under a [not declared](#) license and was authored, remixed, and/or curated by LibreTexts.