BEC

1

Corporate Governance and Financial Risk Management

Module

NOTES

Module 1

Internal Control Frameworks

BEC 1

1 Introduction to COSO

The Committee of Sponsoring Organizations (COSO), an independent private sector initiative, was initially established in the mid-1980s to study the factors that lead to fraudulent financial **reporting**. The private "sponsoring organizations" include the five major financial professional associations in the United States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Financial Executives Institute (FEI), the Institute of Internal Auditors (IIA), and the Institute of Management Accountants (IMA).

In 1992, COSO issued *Internal Control—Integrated Framework* ("the framework") to assist organizations in developing comprehensive assessments of internal control effectiveness.

In 2013, the framework received an update to deal with changes in technology, business models, globalization, outsourcing, and regulatory environment. One significant enhancement to the 2013 update was the formalization of fundamental concepts that were part of the original 1992 framework. Specifically, these fundamental concepts have evolved into 17 principles that have been categorized within the five major internal control components. COSO's framework is widely regarded as an appropriate and comprehensive basis to document the assessment of internal controls over financial reporting.

2 COSO Internal Control Framework

The framework is used by company *management* and its board of directors to obtain an initial understanding of what constitutes an effective system of internal control and to provide insight as to when internal controls are being properly applied within the organization. The framework also provides confidence to external stakeholders that an organization has a system of internal control in place that is conducive to achieving its objectives.

Pass Key

An effective system of internal control requires more than adherence to policies and procedures by management, the board of directors, and the internal auditors. It requires the use of judgment in determining the sufficiency of controls, in applying the proper controls, and in assessing the effectiveness of the system of internal controls. The principles-based approach of the framework supports the emphasis on the importance of management judgment.

2.1 Definition of Internal Control

Internal control is a process that is designed and implemented by an organization's management, board of directors, and other employees to provide reasonable assurance that the organization will achieve its operating, reporting, and compliance objectives.

2.2 Application to Management and Board

The framework assists an entity's management and board of directors in the following areas:

- Effectively applying internal control within the overall organization, on a divisional (operating) unit level or at a functional level.
- Determining the requirements of an effective system of internal control by ascertaining whether the components and principles exist and are functioning properly.
- Allowing judgment and flexibility in the design and implementation of the system of internal control within all operational and functional areas of the organization.
- Identifying and analyzing risks and then developing acceptable actions to mitigate or minimize these risks to an acceptable level.
- Eliminating redundant, ineffective, or inefficient controls.
- Extending internal control application beyond an organization's financial reporting.

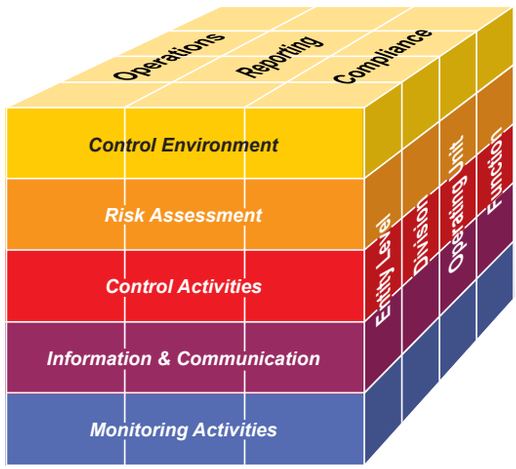
2.3 Application to Stakeholders

The framework also provides value to external stakeholders and other parties that interact with the organization by providing:

- Greater understanding of what constitutes an effective system of internal controls.
- Greater confidence that management will be able to eliminate ineffective, redundant, or inefficient controls.
- Greater confidence that the board has effective oversight of the organization's internal controls.
- Improved confidence that the organization will achieve its stated objectives and will be capable of identifying, analyzing, and responding to risks affecting the organization.

2.4 COSO Cube

The 2013 framework continues to use a cube to depict the relationship between an entity's objectives, integrated internal control components, and organizational structure. The three categories of *objectives* (operations, xreporting, and compliance) are shown as columns on the cube, and the five *internal control components* (control environment, risk assessment, control activities, information and communication, and monitoring activities) are depicted as rows. Additionally, the entity's *organizational structure* (entity level, division, operating unit, and function) is shown on the cube as a third dimension.



Internal Control—Integrated Framework, © 2013 Committee of Sponsoring Organizations of the Treadway Commission (COSO). Used with permission.

2.5 Framework Objectives

There are three *categories of objectives* within the framework.

1. **Operations Objectives**

   Operations objectives relate to the effectiveness and efficiency of an entity's operations. This category includes financial and operational performance goals as well as ensuring that the assets of the organization are adequately safeguarded against potential losses.

2. **Reporting Objectives**

   Reporting objectives pertain to the reliability, timeliness, and transparency of an entity's external and internal financial and nonfinancial reporting as established by regulators, accounting standard setters, or the firm's internal policies.

3. **Compliance Objectives**

   Compliance objectives are established to ensure the entity is adhering to all applicable laws and regulations.

2.6 Components of Internal Control (**CRIME**)

The updated framework retained the original five integrated *components* of internal control, including the control environment, risk assessment, information and communication, monitoring activities, and (existing) control activities. These components and the 17 related fundamental principles are needed to achieve the three *objectives* of internal control.

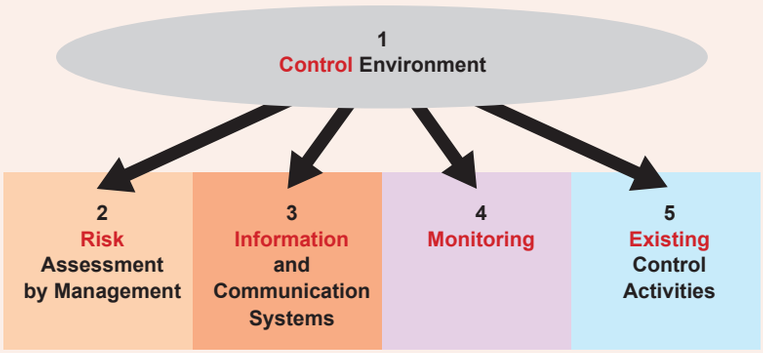
Each of the 17 principles is intended to be suitable to all entities and is presumed to be relevant. However, management may determine that a principle is not relevant to a component.

In addition, the framework introduces 81 points of focus. Some points of focus may not be suitable or relevant, and others may be identified. They are intended to facilitate designing, implementing, and conducting internal control by providing examples. They are not intended to be used as a checklist, and there is no requirement to separately assess whether points of focus are in place.

Pass Key

The COSO framework does not prescribe which controls an entity should implement for effective internal control. Instead, an organization's selection of controls requires management's judgment based on factors unique to the entity.

Illustration 1 Components of Internal Control (CRIME)



Pass Key

Remember that it would be a **CRIME** if you forgot the five components of internal control:

- **Control** Environment
- **Risk** Assessment
- **Information** and Communication
- **Monitoring**
- (**Existing**) Control Activities

2.6.1 Control Environment

The control environment includes the processes, structures, and standards that provide the foundation for an entity to establish a system of internal control. The importance of internal control and expected standards of conduct is established through a "tone at the top" approach taken by the senior management and board of directors of an entity. The five principles related to the control environment are:

1. **Commitment to Ethics and Integrity:** There is a commitment to ethical values and overall integrity throughout the organization. Points of focus include setting the tone at the top, establishing standards of conduct, evaluating adherence to standards of conduct, and addressing deviations in a timely manner.
2. **Board Independence and Oversight:** The board is independent from management and oversees the development and performance of internal control. Points of focus include establishing oversight responsibilities and providing oversight for the system of internal control.
3. **Organizational Structure:** Management establishes an organizational structure. Points of focus include establishing reporting lines, as well as defining, assigning, and limiting authorities and responsibilities that are appropriate to the organization's objectives.

4. **Commitment to Competence:** There is a commitment to hire, develop, and retain competent employees. Other points of focus include evaluating competence and addressing shortcomings in addition to succession planning.
5. **Accountability:** Individuals are held accountable for their internal control responsibilities. Points of focus include establishing performance measures, incentives, and rewards, and evaluating those for ongoing relevance while considering excessive pressures.

2.6.2 Risk Assessment

Risk assessment is an entity's identification and analysis of risks to the achievement of its objectives. The four principles related to risk assessment are:

1. **Specify Objectives:** The organization creates objectives that allow for identification and assessment of the risks related to those objectives. Points of focus include identifying objectives that reflect management's choices while complying with applicable accounting standards, laws, and regulations.
2. **Identify and Analyze Risks:** The organization identifies risks across the entity and analyzes risks in order to determine how the risks should be managed. Points of focus include analyzing internal and external factors, involving appropriate levels of management and determining how to respond to risks.
3. **Consider Potential for Fraud:** The organization considers the potential for fraud in assessing risks. Points of focus include assessing incentives and pressures, opportunities and attitudes, and rationalizations.
4. **Identify and Assess Changes:** The organization identifies and assesses changes that could significantly affect the system of internal control. Points of focus include assessing changes in the external environment, business model, and leadership.

2.6.3 Information and Communication

Information and communication systems support the identification, capture, and exchange of information in a timely and useful manner. The three principles related to information and communications are:

1. **Obtain and Use Information:** The organization obtains or generates and uses relevant, high-quality information to support the functioning of internal control. Points of focus include management identifying and defining information requirements within the internal control component level.
2. **Internally Communicate Information:** The organization internally communicates information necessary to support the functioning of internal controls, including relevant objectives and responsibilities. Points of focus include the flow of information up, down, and across the organization using a variety of methods and channels.
3. **Communicate With External Parties:** The organization communicates with external parties regarding matters that affect the functioning of internal control. Points of focus include management having open, two-way external communication channels using a variety of methods and channels.

2.6.4 Monitoring Activities

Monitoring is the process of assessing the quality of internal control performance over time by assessing the design and operation of controls on a timely basis and taking the necessary corrective actions. The two principles related to monitoring activities are:

1. **Ongoing and/or Separate Evaluations:** The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. One point of focus is to consider establishing baseline understandings.

2. **Communication of Deficiencies:** The organization evaluates and communicates internal control deficiencies in a timely manner to parties responsible for taking corrective action. One point of focus is monitoring corrective actions.

2.6.5 (Existing) Control Activities

Control activities are set forth by an entity's policies and procedures to ensure that the directives initiated by management to mitigate risks are performed.

Control activities may be detective or preventive in nature and may include automated and manual activities (e.g., approvals, reconciliations, verifications). Segregation of duties is usually part of the control activities developed by an organization, and when not practical, management should develop alternative controls. The three principles related to control activities are:

1. **Select and Develop Control Activities:** The organization selects and develops control activities that contribute to the mitigation of risks to acceptable levels. Points of focus include integrating with risk assessment when selecting activities and considering entity-specific factors.
2. **Select and Develop Technology Controls:** The organization selects and develops general control activities over technology to support the achievement of objectives. Points of focus include determining dependencies between the use of technology in business processes and establishing relevant technology infrastructure control activities.
3. **Deployment of Policies and Procedures:** The organization deploys control activities through policies that establish what is expected and procedures that put policies into action. Points of focus include establishing responsibility and accountability for executing policies and procedures and taking corrective action.

Pass Key

The candidate should be familiar with the five components of internal control (in bold) and each of the 17 principles within the components.

Control Environment

- Commitment to ethical values and integrity
- Board independence and oversight
- Organizational structure
- Commitment to competence
- Accountability

Risk Assessment

- Specify objectives
- Identify and analyze risks
- Consider the potential for fraud
- Identify and assess changes

(continued)

(continued)

Information and Communication

- Obtain and use information
- Internally communicate information
- Communicate with external parties

Monitoring Activities

- Ongoing and/or separate evaluations
- Communication of deficiencies

(Existing) Control Activities

- Select and develop control activities
- Select and develop technology controls
- Deploy through policies and procedures

Illustration 2 COSO Application

- **Risk:** Management is unaware of risks that could affect the company.
  - **Component:** Risk assessment.
  - **Principle:** The company identifies risks to achieving its objectives and analyzes risks to determine how the risks should be managed.
  - **Control Activity:** Periodic risk assessments are reviewed by management, including internal audit assessments.
- **Risk:** Employees act in an unethical or unlawful manner.
  - **Component:** Control environment.
  - **Principle:** The company demonstrates a commitment to integrity and ethical values.
  - **Control Activity:** A code of conduct or ethics policy exists and includes provisions about conflicts of interest, related party transactions, illegal acts, and the monitoring of the code by management, the audit committee, and board of directors.

2.7 Effective Internal Control

2.7.1 General Requirements

The framework indicates that an effective system of internal control provides reasonable assurance that the entity's objectives will be achieved. Under the framework, an effective system of internal control requires:

- All five components and 17 principles that are relevant to be both *present* and *functioning*.
  - **Present (Design):** The term "present" means that the components and relevant principles are included in the design and implementation of the internal control system.
  - **Functioning (Operating Effectively):** The term "functioning" demonstrates that the components and relevant principles are currently operating as designed in the internal control system.
- That all five components operate together as an *integrated* system in order to reduce, to an acceptable level, the risk that the entity will not achieve its objectives.

2.7.2 Specific Requirements

To be considered an effective system of internal control, senior management and the board must have reasonable assurance that the entity:

- Achieves effective and efficient operations when:
  - external threats are considered unlikely to have a significant impact on the achievement of objectives; or
  - the organization can reasonably predict and mitigate the impact of external events to an acceptable level.
- Understands the extent to which operations are managed effectively and efficiently when:
  - external events may have a significant impact on the achievement of objectives; or
  - the organization can reasonably predict and mitigate the impact of external events to an acceptable level.
- Complies with all applicable rules, regulations, external standards, and laws.
- Prepares reports that are in conformity with the entity's reporting objectives and all applicable standards, rules, and regulations.

Pass Key

The framework requires judgment in designing, implementing, and conducting internal control and in assessing the effectiveness of internal control.

2.7.3 Ineffective Internal Control: COSO

Internal control deficiencies are shortcomings in a component or components and relevant principles that reduce the likelihood of an entity achieving its objectives.

Although U.S. GAAS uses the terms "significant deficiency" and "material weakness," the COSO framework uses the term "major deficiency."

A major deficiency represents a material internal control deficiency, or combination of deficiencies, that significantly reduces the likelihood that an organization can achieve its objectives.

When a major deficiency is identified pertaining to the presence and functioning of a component or relevant principle, or with respect to the components operating together in an integrated manner, the entity may not conclude that it has met the requirements for an effective internal control system under the COSO framework.

2.8 Internal Control (Framework) Limitations

Although internal control provides reasonable assurance that a firm will achieve its stated objectives, it does not prevent bad decisions or eliminate all external events that may prevent the achievement of the entity's operational goals. The following are inherent limitations that may exist even in an effective internal control system:

- Breakdowns in internal control due to errors or human failure
- Faulty or biased judgment used in decision making
- Issues relating to the suitability of the entity's objectives
- External events beyond the control of the entity
- Circumvention of controls through collusion
- Management override of internal controls

Question 1 **MCQ-06748**

The external auditors for the Horace Company assess the achievement of internal control objectives each year and communicate the assessment to management and the board. Communication by the external auditor illustrates which principle of the information and communication component of the Committee of Sponsoring Organizations' Integrated Framework?

a. Financial Reporting Information
b. Internal Control Information
c. Internal Communication
d. External Communication

Question 2 **MCQ-06483**

A company that retains a CPA with the appropriate knowledge, skills, and abilities to prepare timely and effective financial reporting is applying the ideas from which principle of effective internal control over financial reporting?

a. Integrity and ethical values
b. Management philosophy and operating style
c. Accountability
d. Financial reporting competencies