PART ONE

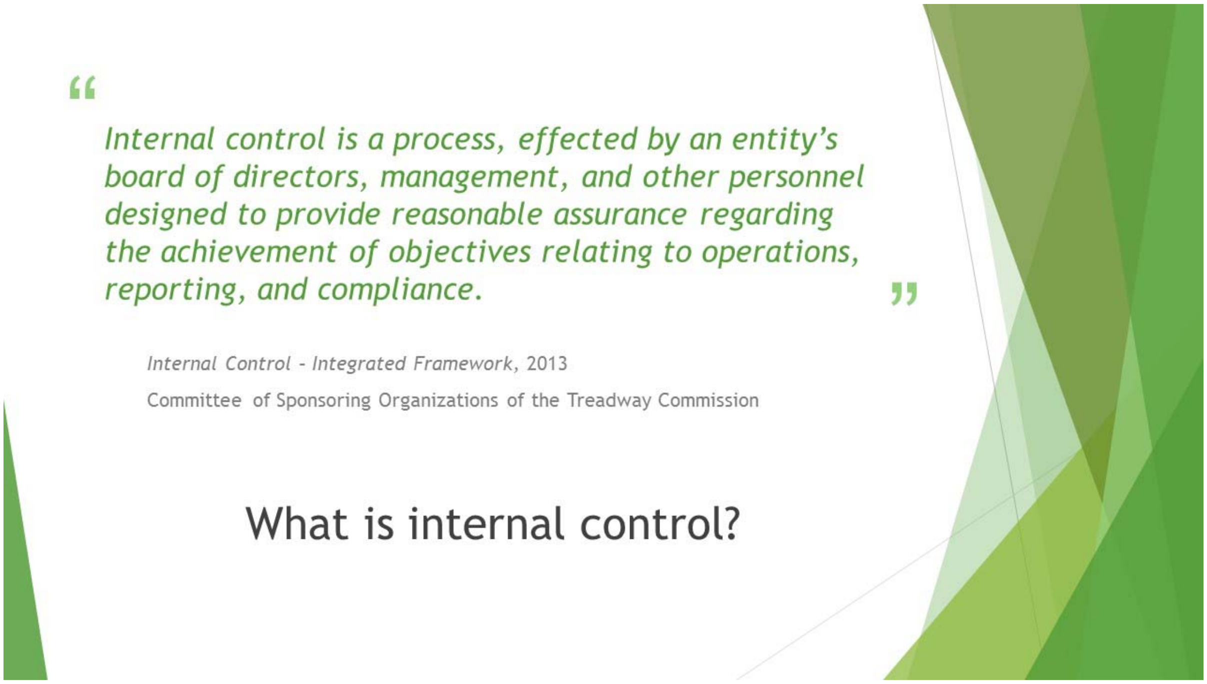
A Basic Introduction to COSO's *Internal Control - Integrated Framework*

Before we answer the question "Who is responsible for what?" with regard to internal control, it's critically important that we have a basic understanding of what a system of internal control is, what its purpose serves, and the components of an effective system of internal control.

The Committee of Sponsoring Organizations of the Treadway Commission updated its *Internal Control – Integrated Framework* document in 2013. The first part of this seminar summarizes its major concepts and lists its components and principles.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal Control – Integrated Framework. Available for purchase or subscription at https://www.cpa2biz.com*

SEMINAR NOTES



> *“Internal control is a process, effected by an entity’s board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.”*

Internal Control - Integrated Framework, 2013

Committee of Sponsoring Organizations of the Treadway Commission

What is internal control?

This definition is intentionally broad in order to (a) capture important concepts that are fundamental to designing, implementing, and assessing internal controls, and (b) to accommodate subsets of internal control, such as a focusing solely on controls over external financial reporting.

The fundamental concepts are:

- Internal control is a **process** (or, more accurately, a series of processes)
- It is effected by **people**
- It provides **reasonable assurance**
- It is **objectives**-focused

It’s important to note that a *system of internal control* is different from an *internal control activity*.

- The system of internal control is the entire process – which is both dynamic and iterative – effected by the organization.
- An internal control activity only a part of the entire process. An internal control activity by itself is of little value. All too often, though, the focus is on the internal control activity and not the entire system.

SEMINAR NOTES

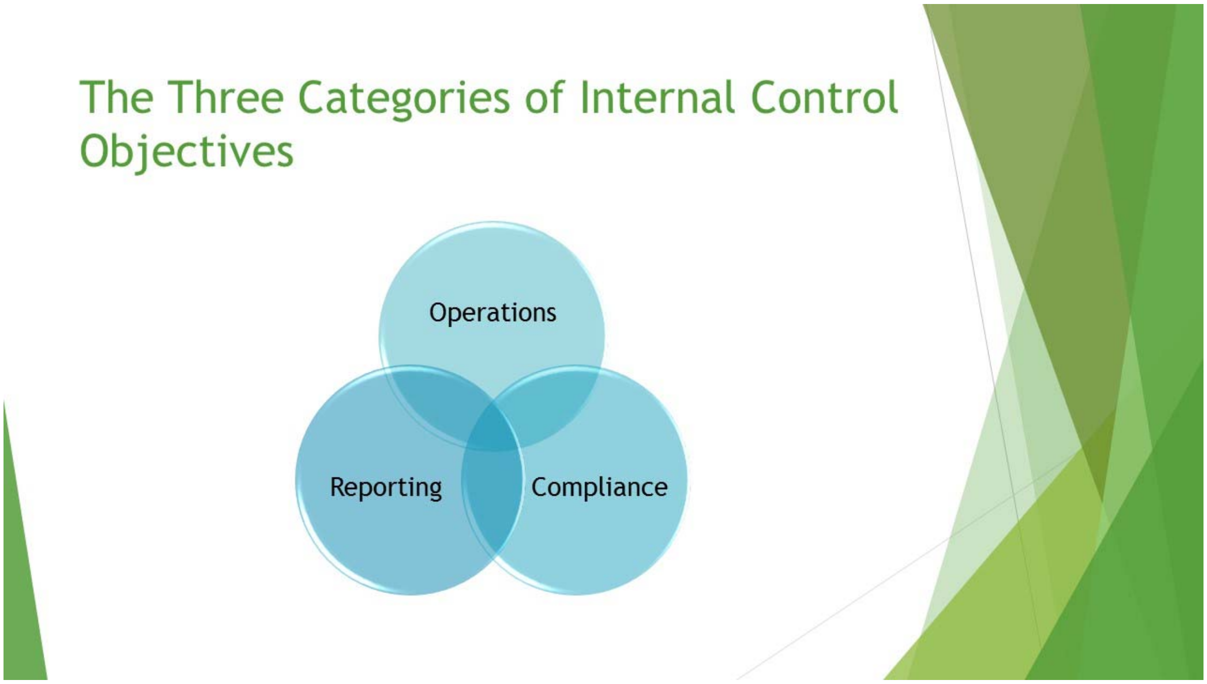
Why is Internal Control Important?

Having a complete system of internal control in place is important because it reduces ***risk*** in achieving objectives.

Risk is simply uncertainty and variability. Therefore, a system of internal control reduces the uncertainty and variability in achieving objectives.

It’s important to note that it does not *eliminate* risk. It merely reduces it. Hence, *reasonable assurance* is used in the definition and not *absolute assurance*.

SEMINAR NOTES



The Three Categories of Internal Control Objectives

Operations

Reporting

Compliance

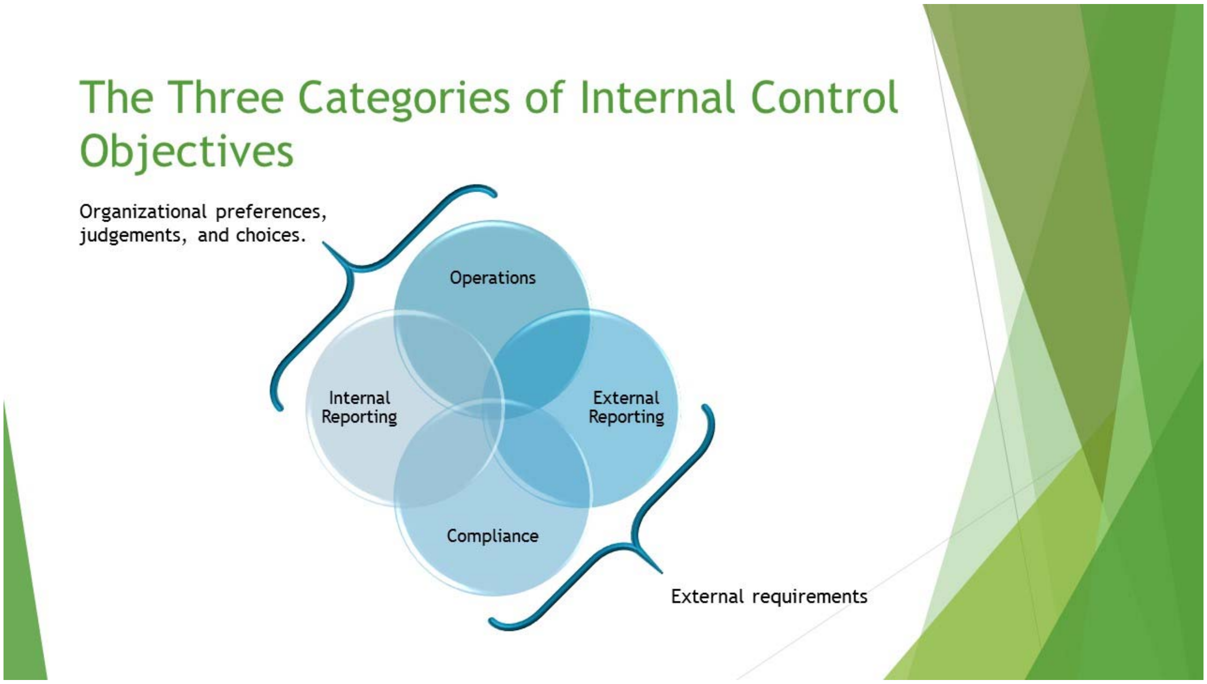
Operational Objectives

- Relate to the achievement of the organization’s basic mission and vision.
- Reflect management’s choices based on the organization’s operating model, its external environment and industry, and the level of performance it wishes to operate at.
- *Safeguarding of Assets* is included as part of an organization’s operational objectives. This includes preventing unauthorized acquisition, use, or disposition of organizational assets. This specific objective is often considered a separate category of objectives. And, if so, the *Framework* can accommodate that, although COSO considers it an operational objective.

Reporting Objectives

- Relate to the preparation of reports for use by the organization internally, external organizations, and stakeholders.
- These are often broken out into sub-categories:
  - Internal Reporting Objectives (Financial and Non-Financial)
  - External Reporting Objectives (Financial and Non-Financial)
- Internal reporting objectives are associated with timely information for management to be able to make decisions and assess performance. Reporting standards are set internally by management and are based on their information needs.
- External reporting objectives are associated with accessing capital markets, acquiring credit, being awarded contracts, reporting to regulators, dealing with suppliers and vendors, and communicating with customers, constituents, and other stakeholders.

SEMINAR NOTES



The Three Categories of Internal Control Objectives

Organizational preferences, judgements, and choices.

Operations

Internal Reporting

External Reporting

Compliance

External requirements

Compliance Objectives

- Related to activities and actions that are governed by laws, rules, and regulations.
- These include well-known laws and regulations, such as those relating to human resources, taxation, and environmental compliance. But, they also pertain to more obscure compliance requirements
- Laws and regulations establish *minimum* standards of conduct. Any additional standards imposed on the organization by the organizations governance and management are considered operational objectives.

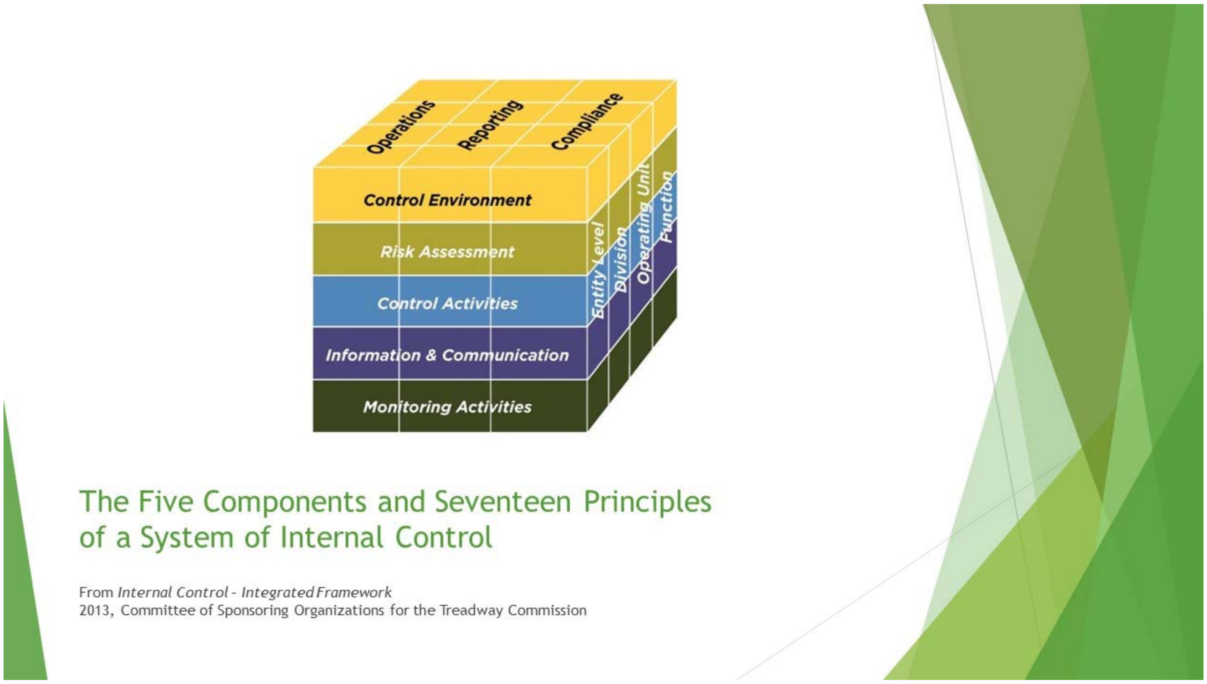
Often there is overlap of objective categories. That is, a particular objective may be simultaneously an operational, reporting, or compliance objective. That's perfectly fine. The key, though, is to understand how that objective relates to and supports each of those categories. Because, while a particular objective may have, say, an operational and reporting function right now. In the future, overall operational goals may shift. That particular objective may no longer be considered an operational objective, but it may still be considered a reporting objective.

Operational and internal reporting objectives are usually based on the organization's preferences, judgements, and choices.

External reporting and compliance objectives are usually based on external requirements.

All objectives, regardless of category, start at the entity level and cascade down to subunits (divisions, operating units, functions) so that the subunits' operational objectives support and contribute to the overall entity-level objectives.

SEMINAR NOTES



The Five Components and Seventeen Principles of a System of Internal Control

From *Internal Control - Integrated Framework*
2013, Committee of Sponsoring Organizations for the Treadway Commission

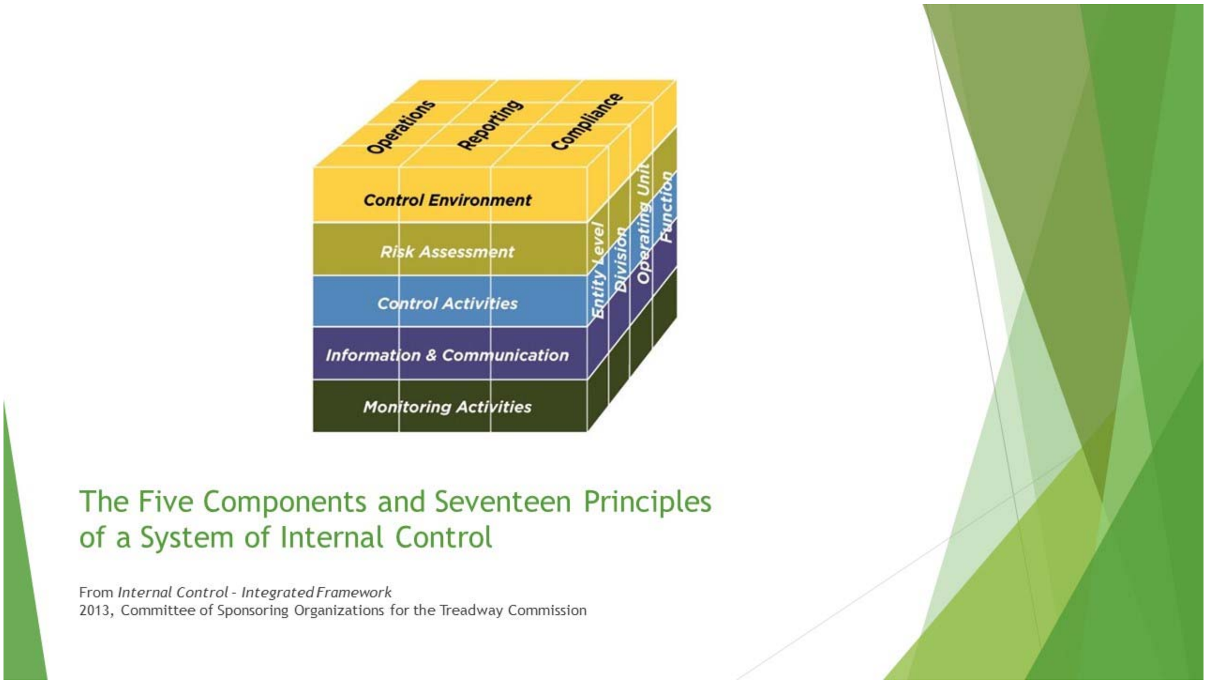
Control Environment

- The organization demonstrates a commitment to integrity and ethical values.
- The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
- The organization considers the potential for fraud in assessing risks to the achievement of objectives.
- The organization identifies and assesses changes that could significantly impact the system of internal control.

SEMINAR NOTES



The Five Components and Seventeen Principles of a System of Internal Control

From *Internal Control - Integrated Framework*
2013, Committee of Sponsoring Organizations for the Treadway Commission

Control Activities

- The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- The organization selects and develops general control activities over technology to support the achievement of objectives.
- The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

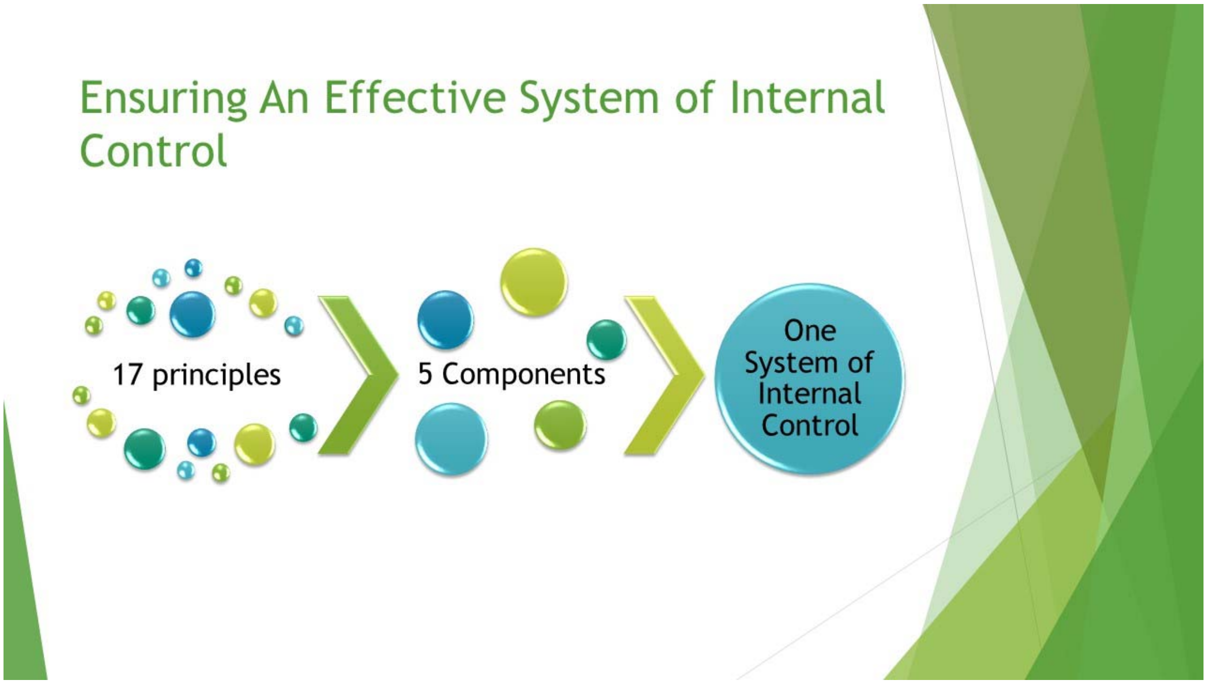
Information and Communication

- The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
- The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
- The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

- The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

SEMINAR NOTES



Ensuring An Effective System of Internal Control

17 principles

5 Components

One System of Internal Control

To be effective, all five components and their relevant principles must be *present and functioning*, and they must be *operating together* in an integrated manner.

- "Present and functioning" means that the components and principles *exist in the design and implementation* of the system of internal control and *continue to exist in the conduct* of the system of internal control.
- "Operating together" means that the components collectively reduce risk.

The *Framework* views **all components** of internal controls as suitable and relevant to all entities. Likewise, because principles are fundamental concepts associated with components and have a significant bearing on the presence and functioning of an associated component, **all seventeen principles** are considered suitable and relevant to all entities. Therefore, if a principle is not present and functioning, the associated component cannot be considered present and functioning.

- Management, with board oversight, may determine that a particular principle is not relevant to the organization. However, this is rare. If it is determined as such, though, the organization must support its determination with the rationale of how, in the absence of that principle, the associated component can be present and functioning.

SEMINAR NOTES

Deficiencies in Internal Control

When a shortcoming exists in a component and relevant principles that reduces the likelihood of achieving organizational objectives (i.e., increases risk), an *internal control deficiency* exists.

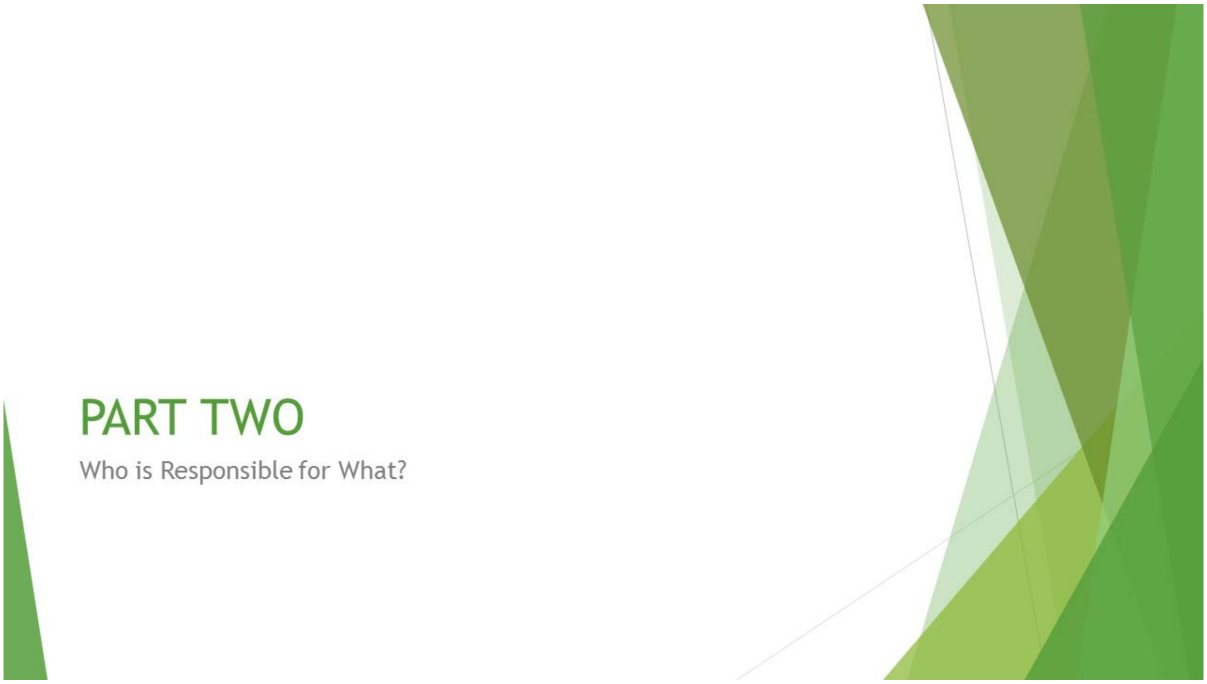
A *major deficiency* is one that severely reduces the likelihood of achieving objectives.

- Whenever a component and one or more relevant principles are not present or functioning or when components are not operating together, a major deficiency automatically exists.
- When a major deficiency exists, management cannot conclude that it has met the requirements for an effective system of internal control

When a system of internal control is effective, management and those charged with governance can be reasonably assured that…

- the organization is achieving **effective and efficient** operations (operations),
- the organization is preparing **reliable** internal and external reports (reporting), and
- the organization is operating in **compliance** with applicable laws and regulations (compliance).

SEMINAR NOTES



PART TWO

Who is Responsible for What?

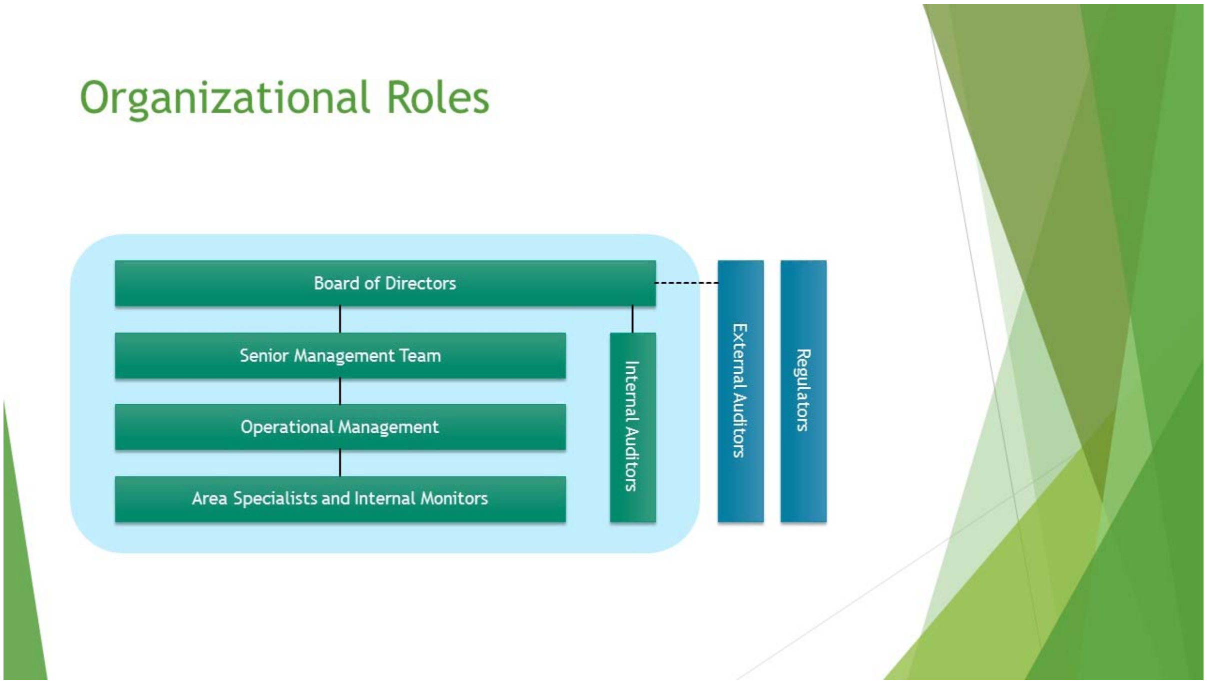
Now that we have a basic understanding of what a system of internal control consists of and how it is designed, we can move on to the seminar's question: Who is responsible for what?

Seeing as the system of internal control is effected by people, those people – the organization's employees – should have a good understanding of what their roles are, where their role fits into the entire organization, and, most importantly, what their responsibilities are.

COSO and the Institute of Internal Auditors released a whitepaper in July 2015 to assist organizations in obtaining a better understanding of roles and responsibilities. This whitepaper, *Leveraging COSO across the Three Lines of Defense*, is summarized the second half of this seminar.

The Institute of Internal Auditors, Anderson, D., and Eubanks, G. (2015). *Leveraging COSO across the Three Lines of Defense.*
Available for download at http://www.coso.org/guidance.htm.

SEMINAR NOTES



Organizational Roles

Board of Directors

Senior Management Team

Operational Management

Area Specialists and Internal Monitors

Internal Auditors

External Auditors

Regulators

Organizations may have unique structures, but most have the following broad categories of roles:

- **Board of Directors** (Board of Trustees, City Councilors, Board of Selectmen, etc., a.k.a. Those Charged with Governance)
- **Senior Management** (CEO, Executive Director, City Administrator, Town Manager, CFO, Director of Finance, CIO, COO, Chief Legal Officer, etc.)
- **Operational Managers** (subunit managers, divisional managers, functional managers, etc.)
- **Area Specialists and Internal Monitors** (information security, physical security, quality control, environmental compliance, legal compliance, supply chain, etc.)
- **Internal Auditors**

SEMINAR NOTES

Board of Directors

Oversight of the Organization

The board is responsible for *overseeing* the system of internal control.

- Establish the overall, long-term objectives of the organization
- Define high-level strategies for achieving objectives
- Establish governance structures to best manage risk
- Define expectations about integrity, ethical values, transparency, and accountability

To execute their responsibilities properly, board members must…

- Have a working knowledge of the organization’s activities and environment
- Commit the time necessary to fulfill their responsibilities
- Maintain open and unrestricted communications with all entity personnel, independent auditors, external reviewers, and legal counsel
- Be objective, capable, and inquisitive

Together with Senior Management, they establish the **Control Environment** component of the system of internal control.

SEMINAR NOTES

Senior Management

Design, Implementation, and Leadership of the System of Internal Control

Senior Management is responsible for *designing, implementing, and leading* an effective system of internal control.

- Provide leadership and direction in shaping organizational values, standards, expectations of competence, organizational structure, and accountability
- Specify entity-wide objectives and policies
- Maintain oversight and control over the risks the organization faces
- Guide the development and performance of control activities at the entity-level
- Communicate expectations and information requirements
- Evaluate control deficiencies and their impact on effectiveness of the system of internal control
- Delegate responsibility for designing, implementing, and assessing more specific internal control procedures to subunit managers.

For functional or operating unit senior management (e.g., CFO, CIO, COO, etc.), they focus on the objectives of their respective units, ensure that they are aligned with entity-wide objectives, and develop and implement internal control policies and procedures to support those objectives.

With board oversight, senior management establishes the **Control Environment** component of the system of internal control.

SEMINAR NOTES

Operational Management

The First Line of Defense

Owners of Risk and Managers of Control

Operational management are front-line and mid-line managers who are responsible for day-to-day *ownership of risk* and *management of control.*

- Design and implement processes to identify and assess significant risks within their operational realm.
- Select and develop internal control activities to respond to identified risks.
- Highlight inadequate processes and address control breakdowns.
- Communicate to key stakeholders of the activity.

Operational management is responsible for the **Risk Assessment**, **Control Activities**, and **Information and Communication** components of the *Framework*. Additionally, in conjunction with the area specialists and internal monitors, they have shared responsibility for the **Monitoring** component.

SEMINAR NOTES

talk
to the
experts

Area Specialists and Internal Monitors

The Second Line of Defense

Ongoing Monitors of Risk and Control

Area specialists and internal monitors are responsible for the *ongoing monitoring* of control and risk.

- Work closely with operating managers to define implementation strategies
- Provide expertise in their respective areas with regard to risk.
- Help identify known and emerging risks
- Assist management in defining which activities to monitor, assist in designing effective controls, provide communication and education about control processes, and explain how to measure success.
- Monitor controls on an ongoing basis to determine whether the controls are functioning as intended.
- Evaluate and communicate deficiencies to operating and senior management and assist in developing corrective actions.

They are part of management and, therefore, are not independent, but they should still exercise an adequate degree of objectivity.

Along with operational management, they are responsible for the **Monitoring** component of the system of internal control.

SEMINAR NOTES

Internal Auditors

The Third Line of Defense

Independent and Objective Assurance

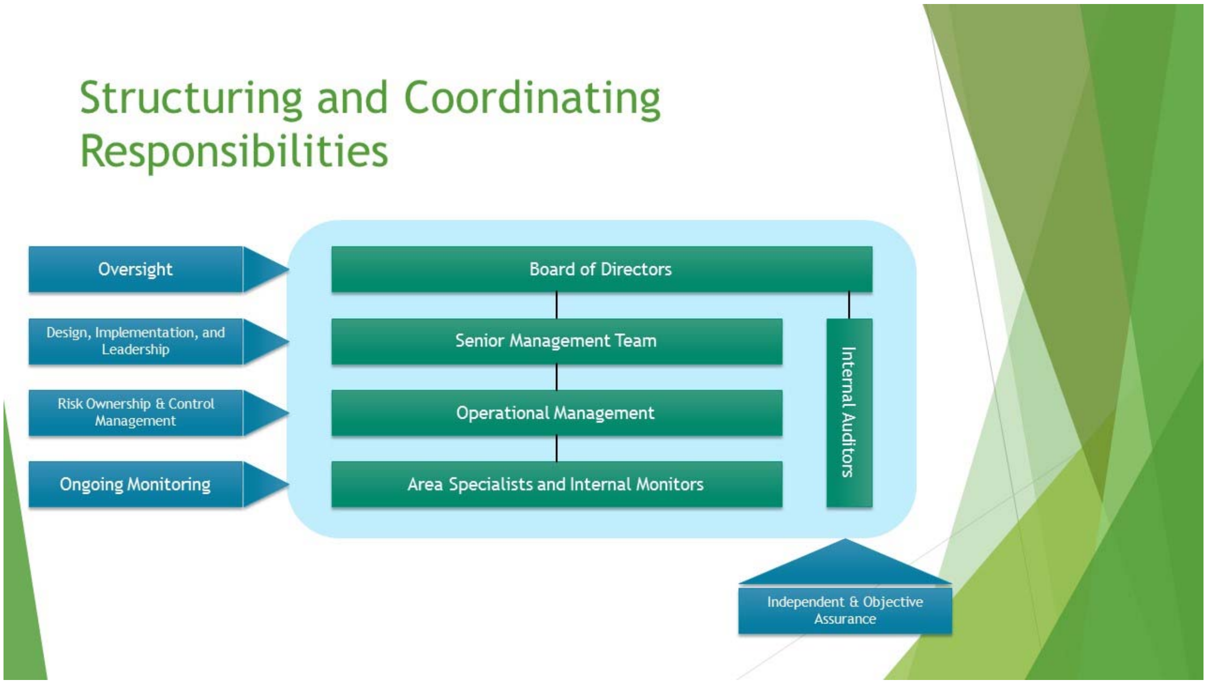
Internal auditors are responsible for providing *independent, objective assurance* to the board and senior management regarding the design, implementation, and effectiveness of the system of internal control.

- They assess all components of the *Framework*
- They have independence from management and have direct communication with the board.
- They provide assurance regarding the efficiency and effectiveness of governance, risk management, and internal control.
- They review all aspects of the organization's operations and activities.

Internal auditors *do not* design or implement controls and *are not* responsible for the organization's operations.

They are responsible for assessing and reporting on all components of the system of internal control.

SEMINAR NOTES



Structuring and Coordinating Responsibilities

Oversight

Design, Implementation, and Leadership

Risk Ownership & Control Management

Ongoing Monitoring

Board of Directors

Senior Management Team

Operational Management

Area Specialists and Internal Monitors

Internal Auditors

Independent & Objective Assurance

The Board and Senior Management set the overall objectives and create a good Control Environment. They are not one of the three lines of defense, but rather they use the three lines of defense to help reduce risk in achieving organizational objectives.

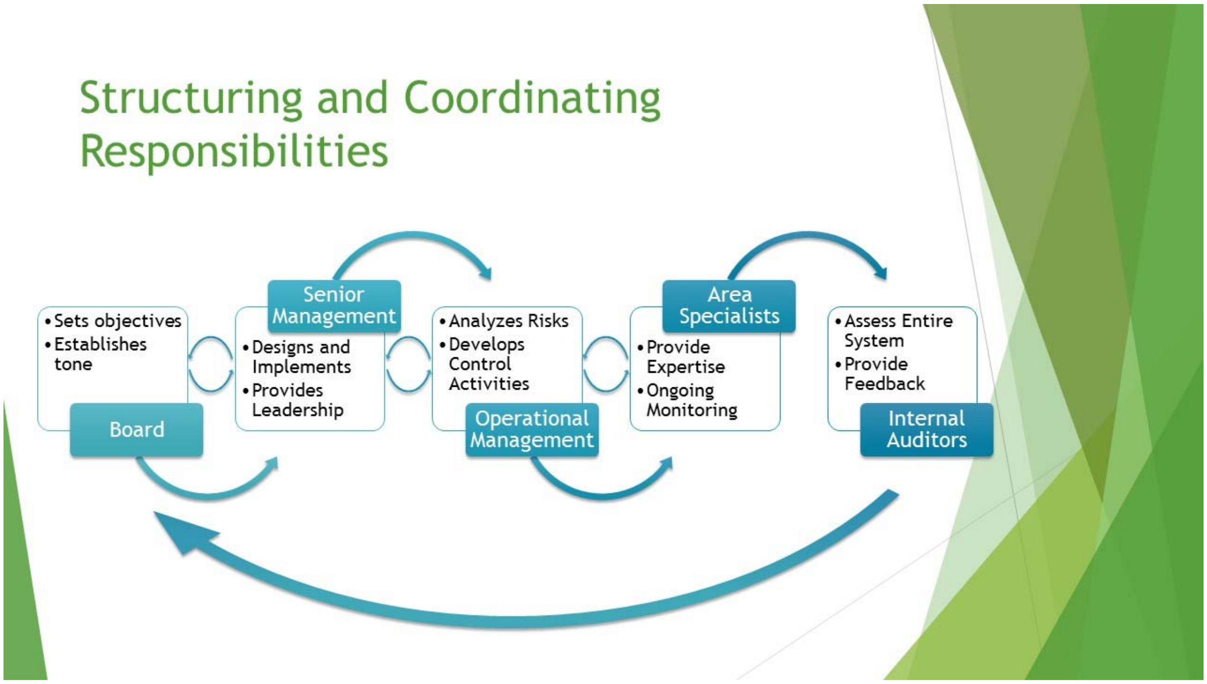
Each level within the organization is accountable to the next higher level for his/her portion of the internal control system.

- Employees who perform control activities (including area specialists and internal monitors) are accountable to operational management.
- Operational management is accountable to senior management.
- Members of senior management are accountable to the CEO.
- The CEO is accountable to the board.
- Internal auditors are accountable to the board.
- And, finally, the board is accountable to its shareholders/citizens.

The “lines of defense” should be as distinct as possible, with roles and responsibilities clearly articulated through policies and procedures and reinforced by a consistent tone at the top and a sound Control Environment.

The Three Lines of Defense Model is designed to be flexible to allow for different sized and differently structured organizations. Therefore, some blending of responsibilities may be okay for some organizations, but the overall aim should be to delineate as much as possible the three lines of defense.

SEMINAR NOTES



Structuring and Coordinating Responsibilities

Board
- Sets objectives
- Establishes tone

Senior Management
- Designs and Implements
- Provides Leadership

Operational Management
- Analyzes Risks
- Develops Control Activities

Area Specialists
- Provide Expertise
- Ongoing Monitoring

Internal Auditors
- Assess Entire System
- Provide Feedback

Coordination should not be confused with structure. While the three lines of defense are separate and have their own unique responsibilities, they should not operate in isolation. The idea is to share information and coordinate efforts regarding risk, control, and governance to achieve the overall organizational objectives.

The best way to ensure sound structure and effective and efficient coordination is for senior management to carefully analyze the organization, assign responsibilities to specific individuals, and communicate those responsibilities through written policies and procedures.

Each person should know their role and *both* the extent and limits of their responsibilities.   That is, there should be no gaps in coverage, but there should be no overlap in coverage either. The former ensures effectiveness, the latter facilitates efficiency.

SEMINAR NOTES

> "Where do our external auditors fit into our system of internal control?"

External auditors and regulators are ***not*** part of an organization's system of internal control.

- They are not part of the organization
- In most cases, they have a limited focus
  - For example, regulators may only be concerned with a particular aspect of the organization, such as controls over expenditures or occupational safety
  - Independent financial statement auditors are primarily concerned with financial reporting controls and place less emphasis on operational and compliance controls (unless they have some bearing on financial reporting controls).

However, they can help boost the overall governance and control structure

- Regulators often have requirements that are intended to strengthen governance and control
- External auditors can provide useful observations about financial reporting risks and related controls.

External auditors and regulators ***should not be considered as substitutes*** for the internal lines of defense and management does not relinquish its responsibilities simply because regulators and external auditors examine and report on aspects of the organization.