COSO

Committee of Sponsoring Organizations of the Treadway Commission

Governance and Internal Control

LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE

By
The Institute of Internal Auditors®

Douglas J. Anderson | Gina Eubanks

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your professional adviser, and this paper should not be considered a substitute for the services of such advisors, nor should it be used as a basis for any decision or action that may affect your organization.

Authors

The Institute of Internal Auditors

Douglas J Anderson, CIA, CPA, CRMA, CMA
Chief Audit Executive Subject Matter Consultant
for the IIA's Audit Executive Center®

Gina Eubanks, CIA, CISA, CRMA, CCSA
Vice President of Professional Services

Acknowledgements

We would like to recognize Richard J. Anderson, Richard Chambers, Sally Dix, Jim DeLoach, Hal Garyn, and Paul Marshall for their help and support in the preparation of this document.

COSO Board Members

Robert B. Hirth, Jr.
COSO Chair

Douglas F. Prawitt
American Accounting Association

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of CPAs (AICPA)

Sandra Richtermeyer
Institute of Management Accountants

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

Governance and Internal Control

LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

July 2015

Copyright © 2015, The Committee of Sponsoring Organizations of the Treadway Commission (COSO).
1234567890 PIP 198765432

All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted or displayed in any form or by any means without written permission. For information regarding licensing and reprint permissions please contact the American Institute of Certified Public Accountants' licensing and permissions agent for COSO copyrighted materials. Direct all inquiries to copyright@aicpa.org or AICPA, Attn: Manager, Rights and Permissions, 220 Leigh Farm Rd., Durham, NC 27707. Telephone inquiries may be directed to 888-777-7077.

Contents

	Page
Introduction	1
Executive Summary	1
I. The Three Lines of Defense Model	2
Roles of Senior Management and the Board of Directors in the Three Lines of Defense Model	4
The First Line of Defense: Operational Management	5
The Second Line of Defense: Internal Monitoring and Oversight Functions	6
The Third Line of Defense: Internal Audit	7
External Auditors, Regulators, and Other External Bodies	9
II. Structuring and Coordinating the Three Lines of Defense	10
Structuring the Three Lines of Defense	10
Coordinating the Three Lines of Defense	11
III. Leveraging COSO across the Three Lines of Defense	13
IV. Conclusion	14
Key Observations	14
Appendix	15
About the Authors	23
About COSO	24
About The IIA	24

Graphics sourced from *The Three Lines of Defense in Effective Risk Management and Control*, The Institute of Internal Auditors, January 2013.

Introduction

This paper is a collaboration between the Committee of Sponsoring Organizations (COSO) and The Institute of Internal Auditors, Inc. The purpose of this paper is to help organizations enhance their overall governance structures by providing guidance on how to articulate and assign specific roles and responsibilities regarding internal control by relating the COSO *Internal Control — Integrated Framework*[1] to the Three Lines of Defense Model.[2]

Executive Summary

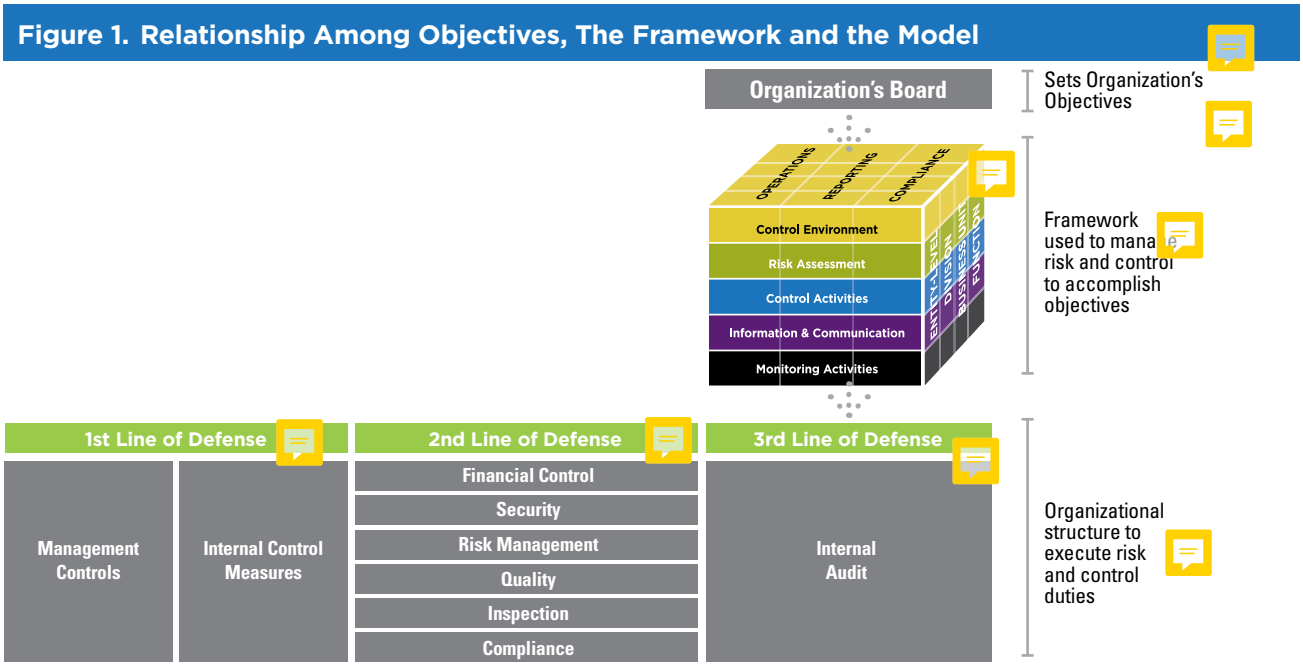
Every organization has objectives it strives to achieve. In pursuit of these objectives, the organization will encounter events and circumstances which may threaten the achievement of these objectives. These potential events and circumstances create risks an organization must identify, analyze, define, and address. Some risks may be accepted (in whole or in part) and some may be fully or partially mitigated to a point where they are at a level acceptable to the organization. There are a number of ways to mitigate risks, with one key method being the design and implementation of effective internal control.

The COSO *Internal Control – Integrated Framework* (the *Framework*) outlines the components, principles, and factors necessary for an organization to effectively manage its risks through the implementation of internal control. However, it is largely silent regarding who is responsible for specific duties outlined in the *Framework*. Clear responsibilities must be defined so that each group understands their role in addressing risk and control, the aspects for which they are accountable, and how they will coordinate their efforts with each other. There should be neither "gaps" in addressing risk and control, nor unnecessary or unintentional duplication of effort.

The Three Lines of Defense (the Model) addresses how specific duties related to risk and control could be assigned and coordinated within an organization, regardless of its size or complexity. Directors and management should understand the critical differences in roles and responsibilities of these duties and how they should be optimally assigned for the organization to have an increased likelihood of achieving its objectives. In particular, the Model clarifies the difference and relationship between the organizations' assurance and other monitoring activities; activities which can be misunderstood if not clearly defined.

As we proceed, we intend to draw from both the *Framework* and the Model with the assumption that the reader has already obtained a basic understanding of the *Framework*. For those who are not familiar with the *Framework*, more information is available at COSO.org. The Model is described in more detail in **Section I**, later in this paper.

Figure 1. Relationship Among Objectives, The Framework and the Model



[1] *Internal Control – Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission (Jersey City, NJ: American Institute of Certified Public Accountants, May 2013. Available at coso.org.

[2] *The Three Lines of Defense in Effective Risk Management and Control*, (Altamonte Springs, FL: The Institute of Internal Auditors Inc, January 2013). Available at: 3LinesofDefenseinEffectiveRiskManagementandControl.

I. The Three Lines of Defense Model

The Model enhances understanding of risk management and control by clarifying roles and duties. Its underlying premise is that, under the oversight and direction of senior management and the board of directors[3], three separate groups (or lines of defense) within the organization are necessary for effective management of risk and control. The responsibilities of each of the groups (or "lines") are:

1. **Own and manage** risk and control (front line operating management).

2. **Monitor** risk and control in support of management (risk, control, and compliance functions put in place by management).

3. **Provide independent assurance** to the board and senior management concerning the effectiveness of management of risk and control (internal audit).

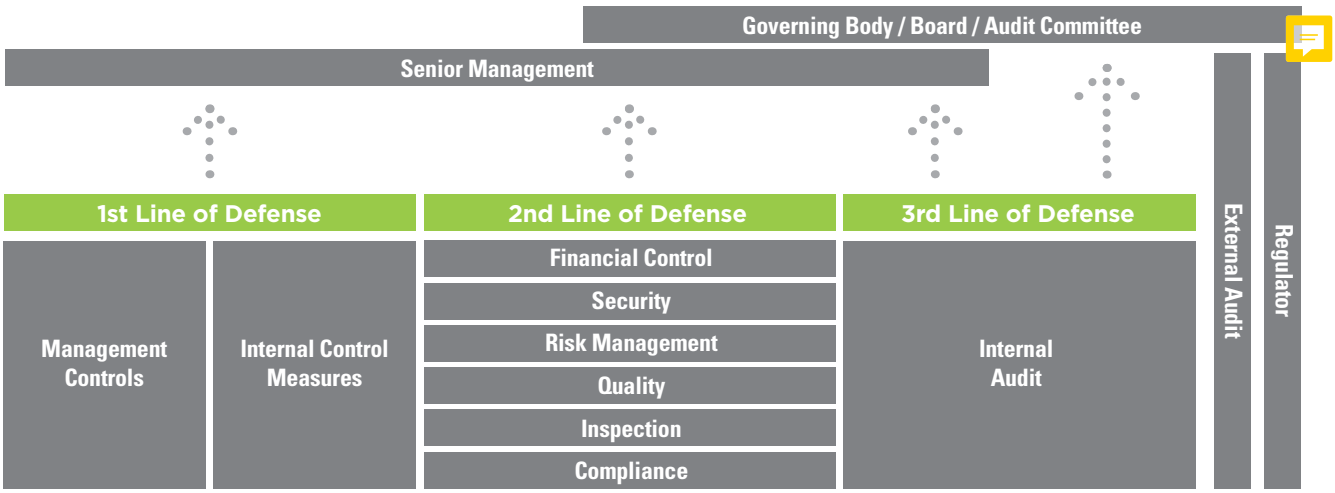
Each of the three lines plays a distinct role within the organization's wider governance framework. When each performs its assigned role effectively, it is more likely the organization will be successful in achieving its overall objectives.

Everyone in an organization has some responsibility for internal control, but to help assure that essential duties are performed as intended, the Model brings clarity to specific roles and responsibilities. When an organization has properly structured the three lines, and they operate effectively, there should be no gaps in coverage, no unnecessary duplication of effort, and risk and control has a higher probably of being effectively managed. The board of directors will have increased opportunity to receive unbiased information about the organization's most significant risks — and about how management is responding to those risks.

The Model provides a flexible structure that can be implemented in support of the *Framework*. Functions within each of the lines of defense will vary from organization to organization, and some functions may be combined or split across the lines of defense. For example, in some organizations, parts of a compliance function in the second line may be involved in designing controls for the first line, while other parts of the second line focus primarily on monitoring these controls.

Figure 2. Three Lines of Defense Model

The Three Lines of Defense in Effective Risk Management and Control, The Institute of Internal Auditors, January 2013



[3] Consistent with other COSO publications, this document uses the term "board of directors" to refer to governing bodies such as boards of directors, boards of trustees, general partners, owners, or supervisory boards.

Regardless of how a particular organization structures its three lines of defense, there are a few critical principles implicit in the Model:

1. The first line of defense lies with the business and process owners whose activities create and/or manage the risks that can facilitate or prevent an organization's objectives from being achieved. This includes taking the right risks. The first line owns the risk, and the design and execution of the organization's controls to respond to those risks.

2. The second line is put in place to support management by bringing expertise, process excellence, and management monitoring alongside the first line to help ensure that risk and control are effectively managed. The second line of defense functions are separate from the first line of defense but are still under the control and direction of senior management and typically perform some management functions. The second line is essentially a management and/or oversight function that owns many aspects of the management of risk.

3. The third line provides assurance to senior management and the board over both the first and second lines' efforts consistent with the expectations of the board of directors and senior management. The third line of defense is typically not permitted to perform management functions to protect its objectivity and organizational independence. In addition, the third line has a primary reporting line to the board. As such, the third line is an assurance not a management function, which separates it from the second line of defense.

The goal for any organization is to achieve its objectives. Pursuit of these objectives involves embracing opportunities, pursuing growth, taking risks, and managing those risks – all to advance the organization. Failure to take the appropriate risks, and failure to properly manage and control risks taken, can prevent an organization from accomplishing its objectives. There is, and always will be, tension between activities to create enterprise value and activities to protect enterprise value. The *Framework* provides a structure to consider risk and control to ensure they are appropriate and properly managed. The Model provides guidance as to an organizational structure to be implemented, assigning roles and responsibilities to parties that will increase the success of effective management of risk and control.

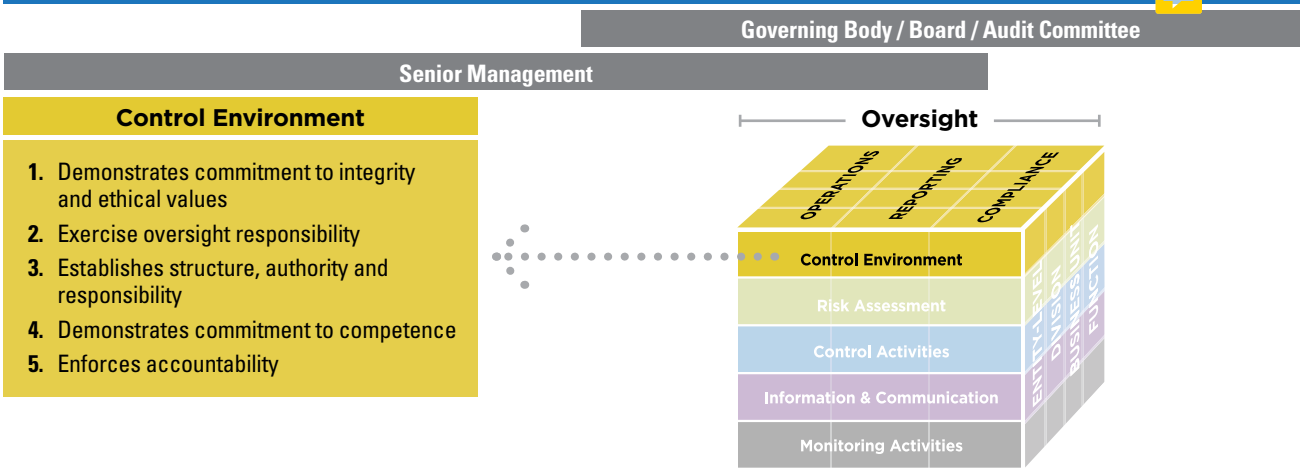
Roles of Senior Management and the Board of Directors in the Three Lines of Defense Model

Senior management and the board of directors have integral roles in the Model. Senior management is accountable for the selection, development, and evaluation of the system of internal control with oversight by the board of directors. Although neither senior management nor the board of directors is considered to be part of one of the three lines, these parties collectively have responsibility for establishing an organization's objectives, defining high-level strategies to achieve those objectives, and establishing governance structures to best manage risk. They are also the parties best positioned to make certain the optimal organizational structure for roles and responsibilities related to risk and control. Senior management must fully support strong governance, risk management and control. In addition, they have ultimate responsibility for the activities of the first and second lines of defense. Their engagement is critical for success of the overall model.

The *Framework* helps to clarify these responsibilities of the board of directors and senior management. As indicated in **Figure 3** below, senior management and the board of directors have primary responsibility for an organization's control environment which is supported by the five principles that establish the tone at the top for the organization.

The Model provides a structure under the *Framework* detailing how roles and responsibilities are assigned. It is best implemented with the active support and guidance of the board of directors and senior management.

Figure 3. Oversight Responsibilities for the Control Environment



The First Line of Defense: Operational Management

The first line of defense in the Model is primarily handled by front-line and mid-line managers who have day-to-day ownership and management of risk and control. Operational managers develop and implement the organization's control and risk management processes. These include internal control processes designed to identify and assess significant risks, execute activities as intended, highlight inadequate processes, address control breakdowns, and communicate to key stakeholders of the activity. Operational managers must be adequately skilled to perform these tasks within their area of operations.

Senior management has overall responsibility for all first line activities. For certain high-risk areas, senior management may also provide direct oversight of front-line and mid-line management, even to the extent of performing some of the first line responsibilities themselves.

Individuals in the first line of defense have significant responsibilities related to the Risk Assessment, Control Activities, and Information/Communication sections of the *Framework*. As indicated in **Figure 4** below, operational managers have primary responsibility for the remaining 12 internal control principles outlined in the *Framework*:

Figure 4. COSO and the 1st Line of Defense

The Second Line of Defense: Internal Monitoring and Oversight Functions

The second line of defense includes various risk management and compliance functions put in place by management to help ensure controls and risk management processes implemented by the first line of defense are designed appropriately and operating as intended. These are management functions; separate from first-line operating management, but still under the control and direction of senior management. Functions in the second line are typically responsible for ongoing monitoring of control and risk. They often work closely with operating management to help define implementation strategy, provide expertise in risk, implement policies and procedures, and collect information to create an enterprise-wide view of risk and control.

The composition of the second line can vary significantly depending on the organization's size and industry. In large, publicly traded, complex, and/or highly regulated organizations, these functions may all be separate and distinct. In smaller, privately owned, less complex and/or less regulated organizations, some of the second-line functions may be combined or nonexistent. For example, some organizations may combine the legal and compliance functions into a single department or may combine a health and safety department with an environmental function. Some or all of the duties of the second line may also be retained by managers within the first line of defense in certain organizations.

Typical second-line functions include specialty expertise groups such as:

- Risk Management
- Information Security
- Financial Control
- Physical Security
- Quality
- Health and Safety
- Inspection
- Compliance
- Legal
- Environmental
- Supply chain
- Other (depending upon industry-specific or company-specific needs)

Under the oversight of management, second-line personnel monitor specific controls to determine whether the controls are functioning as intended. Monitoring activities performed by the second line typically cover all three categories of objectives as described by the *Framework*: operational, reporting, and compliance.

The responsibilities of individuals within the second line of defense vary widely but typically include:

- Assisting management in design and development of processes and controls to manage risks.
- Defining activities to monitor and how to measure success as compared to management expectations.
- Monitoring the adequacy and effectiveness of internal control activities.
- Escalating critical issues, emerging risks and outliers
- Providing risk management frameworks.
- Identifying and monitoring known and emerging issues affecting the organization's risks and controls.
- Identifying shifts in the organization's implicit risk appetite and risk tolerance.
- Providing guidance and training related to risk management and control processes.

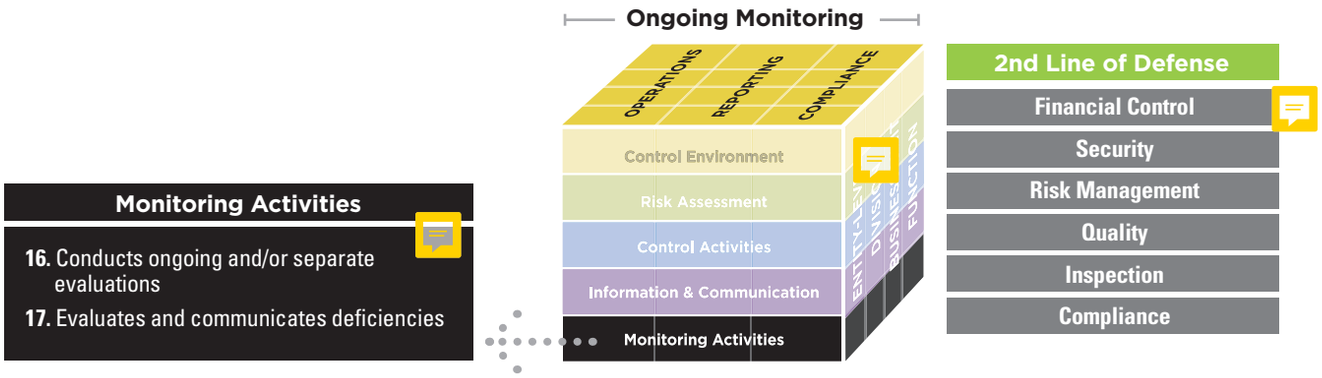
Monitoring by the second line of defense should be tailored to fit the specific needs of the organization. Typically, these activities are separate from day-to-day operational activities. In many cases, monitoring activities are dispersed throughout the organization. In some organizations, however, monitoring functions may be limited to a single or a few areas.

The composition of the second line can vary significantly depending on the organization's size and industry.

Each second-line function has some degree of independence from activities constituting first line of defense, but they are by nature, still management functions. Second-line functions may directly develop, implement, and/or modify internal control and risk processes of the organization. They may also take a decision-making role for certain operational activities. To the extent that the role of second-line functions require them to be directly involved in a first-line activity, that function may not be fully independent from that first line of defense activity.

While not independent, the importance of strong, capable second-line functions cannot be overstated. They are expected to operate with an adequate degree of objectivity and provide important and useful information to senior management and the board of directors regarding the management of risk and control by the first line of defense. They may also provide entity-wide risk and control information to senior management and the board of directors that would not be expected from the first line. To be effective as a line of defense, it must have sufficient stature with leaders and operating management across the organization. Stature comes from the authority and direct reporting lines that command respect.

Figure 5. COSO and the 2nd Line of Defense



The Third Line of Defense: Internal Audit

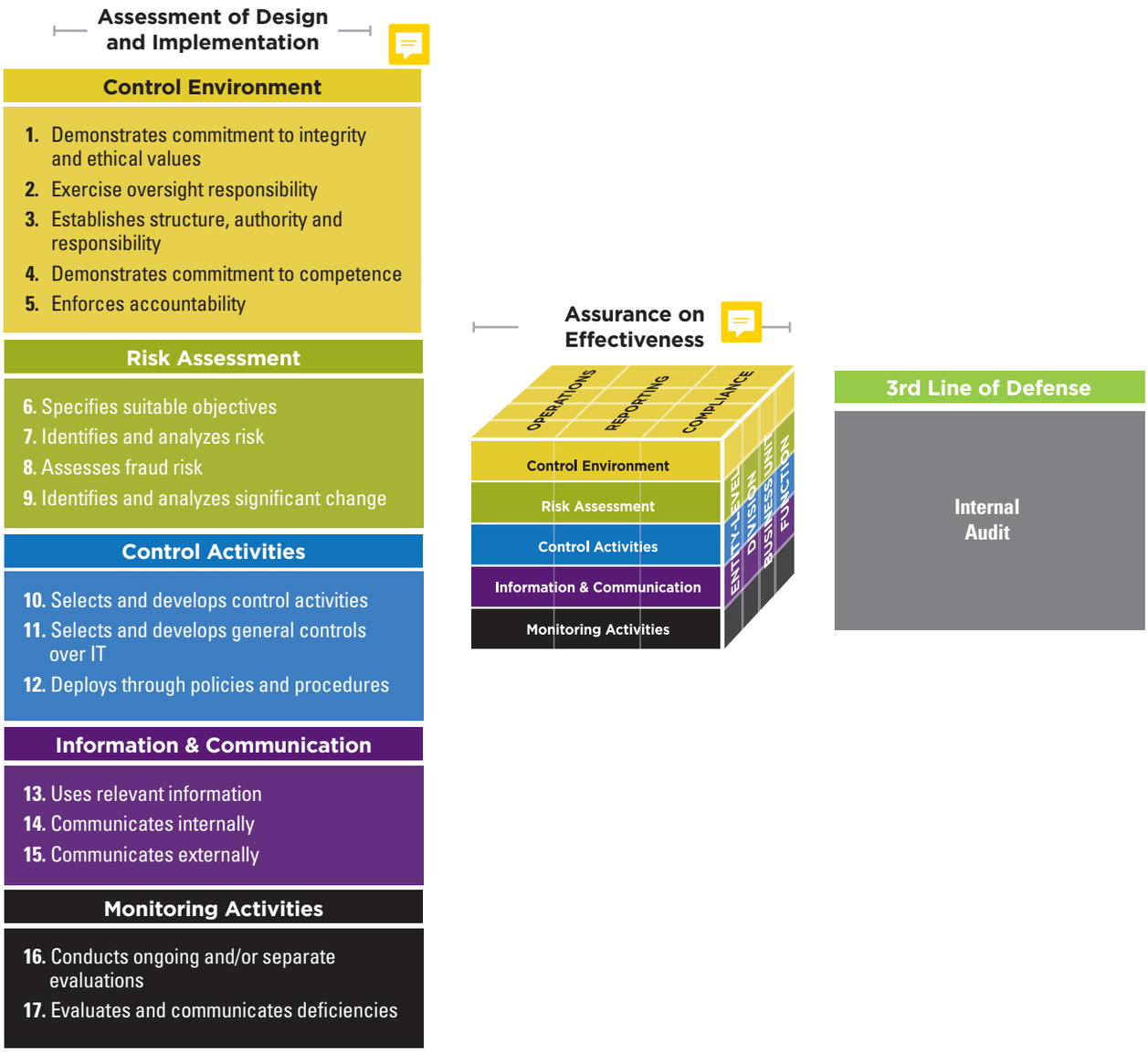
Internal auditors serve as an organization's third line of defense. The IIA defines internal auditing as an "independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."[4]

Among other roles, internal audit provides assurance regarding the efficiency and effectiveness of governance, risk management, and internal control. The scope of internal audit work can encompass all aspects of an organization's operations and activities.

[4] *International Professional Practices Framework (IPPF)®*, (Altamonte Springs, FL: The Institute of Internal Auditors Inc, 2013), 2. Also available at na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx.

What distinguishes internal audit from the other two lines of defense is its high level of organizational independence and objectivity. Internal auditors do not design or implement controls as part of their normal responsibilities and are not responsible for the organization's operations. In most organizations, internal audit independence is further strengthened by a direct reporting relationship between the chief audit executive and the board of directors. Because of this high level of organizational independence, internal auditors are optimally positioned for providing reliable and objective assurance to the board of directors and senior management regarding governance, risk, and control.

Figure 6. COSO and the 3rd Line of Defense



Internal audit actively contributes to effective organizational governance providing certain conditions fostering its independence and professionalism are met. Establishing a professional internal audit activity should therefore be a priority for all organizations. This is important not just for larger organizations but also for smaller entities. Smaller organizations may face equally complex environments with a less formal, robust organizational structure to ensure the effectiveness of governance and risk management processes, and may lack an effective second line of defense. Every organization should establish and maintain an independent, adequate, and competent internal audit staff; reporting to a sufficiently high level in the organization to be able to perform its duties independently; and operating in accordance with a suitable globally recognized set of standards (such as The IIA's *International Standards for the Professional Practice of Internal Auditing*.

External Auditors, Regulators, and Other External Bodies

Although external parties are not formally considered to be among an organization's three lines of defense, groups such as external auditors and regulators often play an important role regarding the organization's overall governance and control structure. Regulators establish requirements often intended to strengthen governance and control, and they actively review and report on the organizations they regulate. Similarly, external auditors may provide important observations and assessments of the organization's controls over financial reporting and related risks.

When coordinated effectively, external auditors, regulators, and other groups outside the organization could be considered as additional lines of defense, providing important views and observations to the organization's stakeholders, including the board of directors and senior management. However, the work of these groups has different and generally more focused or narrow objectives, such that the areas addressed are less extensive than those evaluated by the organization's internal lines of defense. For example, specific regulatory audits may focus solely on compliance issues, safety, or other limited-scope issues; while the three lines of defense are intended to address the entire range of operational, reporting, and compliance risks facing an organization. Parties such as external auditors and regulators, while they contribute valuable information, should not be considered as substitutes for the internal lines of defense as it is an organization's responsibility to manage its risks, not an outside party's responsibility.

II. Structuring and Coordinating the Three Lines of Defense

Structuring the Three Lines of Defense

The Three Lines of Defense Model is purposely designed to be flexible. Each organization should implement the model in a way that is suitable for their industry, size, operating structure, and approach to risk management. However, the overall governance and control environment normally is strongest when there are three separate and clearly defined lines of defense. Organizations should strive to implement a governance structure that is consistent with the Model such that all three lines exist in some form, regardless of size or complexity of the organization. The "lines" should be distinct, with separate roles and responsibilities, clearly articulated in the appropriate policies and procedures of the organization, and reinforced by a consistent "tone from the top."

Exactly where lines are drawn will vary depending upon each organization's specific needs. In some situations, such as some smaller companies or where certain of the functions are in transition, the lines of defense may not be clearly separated. For example, when first starting a risk management function, some organizations may use another function as the catalyst for implementation. In situations where the functions of different lines are not clearly separated, however, the board of directors should carefully consider the potential impacts of the structure. Where possible, these situations where the lines of defense are not clearly separated should be short-term and as functions mature, the appropriate separation should be established. If longer than short-term or temporary, the board of directors should understand the impact of not separating management and assurance functions through the failure to maintain three separate lines of defense.

When considering or assigning specific duties and coordinating among the organization's various risk and control functions, it can be helpful to keep in mind the underlying role of each group in the model.

Figure 7. Differences Between the Three Lines of Defense

Management Functions		Assurance
1st Line of Defense	2nd Line of Defense	3rd Line of Defense
Operating Management	Limited Independence Reports Primarily to Management	Internal Audit Greater Independence Reports to Governing Body

Because organizational independence and objectivity are essential hallmarks of the third line of defense, particular care should be taken if the organization combines the internal auditing function with any second line of defense roles. If the internal audit function is combined with any of the second line functions, senior management and the board of directors should make certain that the functions are not combined or coordinated in a manner that could compromise the organizational independence or objectivity of the internal audit function. Internal auditors normally should not assume any managerial responsibilities for operations that they audit; and in organizations where internal audit is involved in second line activities, this involvement should generally be short term with conflicting roles allocated to different individuals or groups. If internal audit's involvement with second line duties is not short term, senior management and the board of directors need to recognize the limitation on the ability of internal audit to provide independent and objective assurance and they may need to turn to external parties for assurance on the specific activities affected.

Coordinating the Three Lines of Defense

The three lines each have the same ultimate objective: help the organization achieve its objectives with effective management of risk. They serve the same ultimate stakeholders, and they often deal with the same risk and control issues. Senior management and board of directors should clearly communicate the expectation that information be shared and activities coordinated among each of the three lines where this supports the overall effectiveness of the effort and does not diminish any of the line's key functions. For example, many organizations have put in place board level or management level risk policies to articulate these expectations.

Coordination and communication is not to be confused with organizational structure. While they have the same objective, each line has its own unique roles and responsibilities. They are separate lines but should not operate in silos. They should share information and coordinate efforts regarding risk, control and governance. In many situations there could be a shared perspective regarding risk and control.

Careful coordination is necessary to avoid unnecessary duplication of efforts while assuring that all significant risks are addressed appropriately. This coordination is so important that under the *Standard 2050*, chief audit executives are specifically required to "share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts."[5]

In operationalizing this coordination, it is critical that the key roles of executives such as a chief risk officer, a chief compliance officer, or a chief audit executive are carefully reviewed and structured so each can accomplish their unique responsibilities while coordinating and communicating with the other risk and control executives.

The first line of defense has primary ownership of risks and the methods used to manage those risks. The second line provides expertise in risk, helps set implementation strategy, and assists in implementation of policies and procedures. While these two lines have different responsibilities for risk and control, it is essential they work together using the same terminology, understand each other's assessment of the organization's risks, and leverage a common set of tools and processes where possible.

[5] *International Professional Practices Framework (IPPF)*®, (Altamonte Springs, FL: The Institute of Internal Auditors Inc, 2013). Also available at na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx.

The organization's internal audit function, the third line of defense, should include in its scope all the organization's significant risk and control activities. Communication with the first and second line of defense functions will help internal audit to use similar risk terminology and understands these two lines of defense's understanding of risk.

Internal audit should also coordinate their efforts with those of the second line of defense. This coordination could take a variety of forms depending on the nature of the organization, the specific work done by each party, the organizational independence of the second line functions, and the expectations by senior management and the board of directors. In some cases internal audit may be able to base a portion of their assessment on work performed by a second line function. In this situation, internal audit should confirm the work is appropriately designed, planned, supervised, documented, and reviewed. The extent of use and level of reliance on the work of other functions will vary based on specific circumstances. Internal audit also needs to pay careful attention to the organizational independence of the second line functions on which they plan to base a portion of their assessment work. As internal audit is structured with organizational independence to provide unbiased and objective assessments, the function performing the work on which internal audit plans to rely should exhibit a sufficiently high level of organizational independence and objectivity. Capability and efficiency are not the only criteria. Capability of the first or second lines of defense to perform work for internal audit does not mean they bring a requisite level of independence and objectivity. Similarly, the capability of internal audit to perform work of the first or second lines does not mean internal audit performing the work of the first or second lines would necessarily preserve the organizational independence and objectivity of internal audit.

To help establish that work can be coordinated efficiently, the internal audit charter should specify that internal audit has the responsibility to assess the performance and effectiveness of the work of other second line of defense functions or any activity provided by a third party.

Coordination may extend beyond the three lines of defense, to include other external parties such as external auditors. Internal auditors may be able to rely on or use the work of other internal or external providers in providing governance, risk management, and control assurance if they have a sufficient understanding of the work performed, the detailed results, and the independence and competency of the external party. Conversely, internal audit work might intentionally be planned and performed to meet the requirements of external parties. Coordinating efforts with external parties can lead to enhanced efficiency; however, chief audit executives and the board of directors should consider the costs as well as the potential benefits of designing internal audit work for the benefit of external parties.

[7] *Making Data Governance Programs More Effective*, deloitte.wsj.com/riskandcompliance/2014/08/04/good-riddance-to-bad-data-data-governance-gains-momentum/.

III. Leveraging COSO across the Three Lines of Defense

The *Framework* defines five components of internal control and 17 principles representing the fundamental concepts associated with these components. The COSO publication, *Internal Control – Integrated Framework* states that because the 17 principles are drawn directly from the five components of internal control, effective internal control can be achieved by applying each of these principles. Management has the responsibility to assign the essential duties related to the 17 principles and confirm duties are performed as intended.

The Appendix provides examples of how responsibility for the 17 principles may be allocated among the three lines of defense. *Internal Control – Integrated Framework* also identifies various "points of focus" related to each of the 17 principles. Since many of the points of focus represent key responsibilities of individuals within the three lines of defense, readers who are familiar with *Internal Control – Integrated Framework* will find that many of the points of focus are reflected throughout the following section.

The information in the Appendix is intended to provide an example of how duties may be allocated among the three lines of defense. Because every organization is unique, organizations may have sound reasons for defining roles and responsibilities differently. Regardless of how duties are assigned within an organization, specific roles and responsibilities regarding all of the 17 principles should be clearly established and communicated to all relevant parties to mitigate gaps in coverage of internal controls and no unnecessary duplication of effort.

IV. Conclusion

Every organization should clearly define responsibilities related to governance, risk and control to help minimize "gaps" in controls and unnecessary duplications of assigned duties related to risk and control. The Three Lines of Defense Model provides an effective way to enhance communications regarding risk and control by clarifying essential roles and duties. The Model can be useful for clarifying how responsibilities regarding risk and control might be coordinated across an organization.

The underlying premise of the Model is that, under the oversight and direction of senior management and the board, three separate groups (or lines of defense) are necessary for effective management of risk and control. The three groups:

- **Own and manage** risk and control (operating management).
- **Monitor** risk and control in support of management (risk, control, and compliance functions put in place by management).
- **Provide independent assurance** about effectiveness of risk management and control to the board and senior management (internal audit).

Each of the three "lines" has a distinct role within the organization's wider governance framework, and when each performs its assigned role effectively, the likelihood of a significant control breakdown is reduced. This structure also supports the board of directors in receiving impartial information about the organization's most significant risks — and about how management is responding to those risks.

The Model can be used in conjunction with the COSO *Internal Control – Integrated Framework* to help ensure individuals within each line of defense understand the full extent of their responsibilities regarding risk and control, and how their duties fit into the organization's overall risk and control structure.

Key Observations

1. Senior management and the board of directors have ultimate responsibility for ensuring the efficiency and effectiveness of governance, risk management, and control processes.
2. Risk management is strongest when there are three separate and clearly identified lines of defense. All three lines of defense should exist in some form at every organization, regardless of size or complexity.
3. Each group within the three lines of defense should have clearly defined roles and responsibilities that are supported by appropriate policies, procedures, and reporting mechanisms.
4. Information should be shared and activities coordinated among each of the lines of defense to improve efficiency and avoid duplication of effort while ensuring all significant risks are addressed appropriately.
5. Lines of defense should not be combined or coordinated in a manner that compromises their effectiveness. Each line of defense has unique positioning in the organization and unique responsibilities. Particular care should be taken if the organization combines functions across the three lines of defense. The effectiveness of the second or third line of defense can be adversely affected if the combination injures the uniqueness of that line. Capability and efficiency are not the only criteria; independence and objectivity are also essential elements to consider.

Appendix

Principle 1. The organization demonstrates a commitment to integrity and ethical values.

1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
All lines of defense should be expected to demonstrate through their directives, actions, and behavior the importance of integrity and ethical values.			
• Leads by example in implementing values, a philosophy and an operating style for the organization. • Implements ethics-related objectives, programs and activities. • Designs and implements processes to evaluate the performance of individuals and teams against expected standards of conduct.	• Specific members of the 2nd Line may be requested to support compliance hotlines, investigate potential wrongdoing, or perform other specific duties related to integrity and ethical values.	• Assesses the state of the organization's ethical climate and the effectiveness of its strategies, tactics, communications, and other processes in achieving the desired level of legal and ethical compliance. • Evaluates the design, implementation, and effectiveness of the organization's ethics-related objectives, programs and activities. • Provides assurance that ethics programs achieve stated objectives, key risks are effectively managed and controls continue to operate effectively. • Provides consulting services to help the organization establish a robust ethics program and improve its effectiveness to the desired performance level.	• The board oversees the ethical climate and ensures management has sound ethics-related programs and objectives. • The board is responsible for establishing effective "tone at the top." This includes communicating expectations regarding integrity, ethical values and standards of conduct.

Principle 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
• Furnishes the board with adequate information regarding development and performance of internal controls to enable the board to fulfill its fiduciary duties.	• Board oversight is supported by structures and processes that management establishes at the business-execution level. This support may be provided by either the first or the second line of defense. For example, either a management committee or a second-line of defense group may focus on topics such as IT or compliance.	• Provides assurance regarding the development and performance of internal controls, evaluating whether or not controls are designed appropriately, implemented effectively, and operating as intended. • May assist the board by suggesting specific agenda items related to Principle 2 for discussion at meetings of the board of directors.	• The board is responsible for ensuring it has sufficient members who are independent from management and objective in evaluations and decision-making. • The board retains oversight responsibility for management's design, implementation, and conduct of internal control: - **Control Environment** – Establishing integrity and ethical values, oversight structures, authority and responsibility, expectations of competence, and accountability to the board. - **Risk Assessment** – Engaging with management to set the risk appetite. Overseeing management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management override of internal control. - **Control Activities** – Providing oversight to senior management in the development and performance of control activities. - **Information and Communication** – Analyzing and discussing information relating to the organization's achievement of objectives. - **Monitoring Activities** – Assessing and overseeing the nature and scope of monitoring activities and management's evaluation and remediation of deficiencies. • The board meets with internal audit, and potentially parties in the second line of defense, independent of management.

Principle 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
• Establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. • Communicates information regarding structures, reporting lines, and authorities and responsibilities to the board, to enable the board to fulfill its oversight responsibilities.	• Work with management, organizational structures, reporting lines, and appropriate authorities and responsibilities appropriate for them to execute their responsibilities.	• Provides assurance regarding the appropriateness and effectiveness of the organization's operational structures, reporting lines, authorities, and responsibilities in the pursuit of objectives. • Implements policies and practices to execute its activities in accordance with its charter including appropriate reporting lines and authorities. • Periodically confirms to the board its organizational independence and objectivity.	• The board approves organizationwide objectives and is responsible for oversight of the development and maintenance of structures, reporting lines, and assignment of appropriate authorities and responsibilities in the pursuit of objectives. • The board issues appropriate charters to establish its committees, including the audit committee. • The audit committee approves appropriate charters for risk and control functions it is responsible for including internal auditing.

Principle 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
• Attracts, develops, and retains competent individuals in alignment with objectives.	• Attracts and develops competent talent to achieve its objectives. • Ensures that its people and activities are appropriately aligned with management. This may include rotating people through various management functions.	• Attracts, develops, and retains individuals competent and skilled to accomplish its mission and charter. • May evaluate and provide assurance regarding efficiency and effectiveness of policies and processes such as: - Human resources policies. - Recruitment practices. - Training and development programs. - Performance evaluation systems. - Compensation plans. - Succession plans.	• The board provides oversight to ensure that management demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. • Board committees ensure that functions it oversees have competent talent. • Board compensation committee ensures that incentive and compensation plans are aligned with the risk appetite and long-term objectives of the organization.

Principle 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
• Holds individuals accountable for their internal control responsibilities in the pursuit of objectives. This responsibility includes communication of specific responsibilities, implementation of performance evaluation systems, and implementation of personnel processes designed to hold individuals accountable for their actions.	• As delegated by management, individuals in the second line of defense monitor and report on fulfillment of specific internal control responsibilities.	• Provides assurance regarding fulfillment of specific internal control responsibilities. • Internal auditors may make recommendations regarding accountability but normally have no direct authority to make decisions regarding personnel actions or other processes designed to hold individuals accountable for their internal control responsibilities.	• The board is responsible for ensuring that management holds individuals accountable for their internal control responsibilities. • The board compensation committee ensures that incentive and compensation plans are aligned with the objectives of the organization.

Principle 6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
All individuals who are part of the system of internal control need to understand the overall strategies and objectives set by the organization.			
• Setting objectives is a key part of the management process related to strategic planning. • With board oversight, sets entity-level objectives that align with the organization's mission, vision, and strategies. • Specifies suitable objectives in adequate detail so that risks to achievement of objectives can be identified and assessed. • Apply tolerances to specific risks. • Links entity-level objectives to more specific sub-objectives that cascade throughout the organization. • Both entity-level objectives and associated sub-objectives should be specific, measurable, attainable, relevant, and time-bound.	• Not responsible for setting or approving entity-level objectives as a whole; but may be called upon to draft, implement, monitor, and report on objectives or sub-objectives related to their specific areas of expertise, such as objectives related to compliance or quality control. • Assess whether appropriate risk appetites and tolerances are considered.	• Verifies that objectives are in place and that they are specific, measurable or observable, attainable, relevant, and time-bound. - Entity-wide reviews of the objective-setting process may be performed as separate stand-alone engagements. - Specific objectives or sub-objectives may also be reviewed during other internal audit engagements. • To maintain internal audit organizational independence, auditors normally do not develop objectives (other than those specific to the internal auditing function.)	• The board has responsibility for oversight of objective-setting, helping to ensure that high-level objectives reflect decisions regarding how the organization seeks to create, preserve, and realize value for its stakeholders. • The board with management establishes appropriate risk tolerances and appetite and ensure that they are communicated across the organization.

Principle 7. 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.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
• Identifies and controls risks related to achievement of objectives. • Defines the organization's risk appetite and tolerances, establishes risk management systems, and establishes accountabilities for controlling specific risks under the board's oversight.	• An enterprise risk management function may be delegated significant responsibilities regarding risks and controls. Typical tasks might include: - Establishing a common risk language or glossary. - Describing the organization's risk appetite and tolerances. - Identifying and describing risks in a "risk inventory." - Implementing a risk-ranking methodology to prioritize risks within and across functions. - Establishing a risk committee and or chief risk officer to coordinate certain activities of other risk management functions. - Establishing ownership for particular risks and responses. - Developing action plans to ensure the risks are appropriately managed. - Developing consolidated reporting for various stakeholders. - Monitoring the results of actions taken to mitigate risk. - Ensuring efficient risk coverage by internal auditors, consulting teams, and other evaluating entities. - Developing a risk management framework that enables participation by third parties and remote employees. • Specific groups such as security and compliance functions may assist management in identifying risks related to their area of expertise, taking into account the risk appetite levels set by management for the different activities or parts of the organization.	• Takes into account organization's risk framework to perform an organizationwide risk-based audit plan. • May facilitate certain enterprise risk management activities as long as independence and objectivity are not impaired. • Considerations to developing an internal audit plan may include: - Identification and assessment of inherent and residual risks. - Mitigating controls, contingency plans, and monitoring activities linked to specific risks. - Accuracy and completeness of risk registers. - Adequacy of documentation regarding management's risk and control activities.	• The board establishes the overall strategy of the organization and its objectives including understanding the risks associated with the strategy. • The board provides oversight and holds management accountable for identifying and managing risks to the achievement of objectives.

Principle 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
• Implements processes to identify, deter and detect fraud. • Reviews the organization's exposures to fraud with the organization's internal and external auditors.	• Ensures that risk and control assessments include the consideration of the risk of fraud. • Groups such as investigations units may play a significant role in deterring and detecting fraud. These groups may be charged with developing and monitoring entity-wide policies and procedures regarding fraud.	• The *Standards* require that internal auditors exercise due professional care by considering the probability of significant fraud in areas under review. • Internal auditors are required to have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.	• The board is responsible for oversight of systems and processes intended to deter and detect fraud. • The board and senior management set the tone for the prevention and detection of fraud. • The board should receive periodic reports on the organization's exposures to fraud including financial reporting fraud.

Principle 9. The organization identifies and assesses changes that could significantly impact the system of internal control.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
Because change can arise from a wide variety of internal and external sources, individuals within all three lines of defense should be alert for emerging issues that could significantly impact the system of internal control.			
• Has primary responsibility for the system of internal control and for identification and assessment of changes that could significantly impact the system of internal control. • Communicates information regarding changes that could significantly impact the system of internal control to the board in sufficient detail to enable the board to fulfill its oversight responsibilities.	• May be asked to assist management with assessments of the impact of changes on the system of internal control. • Needs to be proactive to adapt to the changes. • Regularly monitors and considers changes to the organization's legal, regulatory and compliance risk.	• Identifies and assesses changes that could significantly impact the system of internal control during periodic risk assessments and throughout the course of internal audit work. • Communicates regularly with management to anticipate changes and the impact on organizational risk assessment.	• The board has responsibility for ensuring that management has established processes to enable identification and assessment of changes that could significantly impact the system of internal control.

Principle 10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
• Maintains effective internal controls and for executing risk and control procedures on a day-to-day basis. Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with established goals and objectives. Through a cascading responsibility structure, mid-level managers design and implement detailed procedures that serve as controls and supervise execution of those procedures by their employees. • Naturally serves as the first line of defense because controls are designed into systems and processes under the guidance of operational management. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdowns, inadequate processes and unexpected events.	• Functions within the second line of defense normally are responsible for monitoring specific controls on behalf of management. • As assigned by management, individuals in the second line of defense may also participate in the selection and development of specific controls; however, management retains responsibility for the system of internal controls.	• Provides assurance that the controls put in place by management are designed appropriately, implemented effectively, and operating as intended to mitigate risks to the achievement of objectives to acceptable levels. • Provides suggestions intended to improve the efficiency and effectiveness of internal controls; however, management retains responsibility for the system of internal controls.	• The board evaluates information and provides oversight to help ensure that management's system of internal control is adequate to mitigate risks to the achievement of objectives to acceptable levels.

Principle 11. The organization selects and develops general control activities over technology to support the achievement of objectives.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
• Designs and implements control activities related to technology. This includes creating and communicating policies and procedures regarding technology and ensuring that IT controls are adequate to support the achievement of objectives. • Establishes processes to monitor and assess developing risk exposures related to new and emerging technology.	• Individuals in the second line of defense often are assigned duties regarding the monitoring of specific technology controls. • Groups such as information security departments may also play significant roles in selecting, developing, and maintaining controls over technology, as designated by management.	• Assesses whether the organization's IT governance processes support the organization's strategies and objectives. • Provide assurances regarding the efficiency, effectiveness, and completeness of technology controls and, as appropriate, may recommend improvements to specific control activities. • To preserve internal audit independence and objectivity, internal auditors normally do not select or develop general control activities over technology; however, they may make recommendations regarding technology controls. • Internal auditors must have sufficient knowledge of key IT risks and controls to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.	• The board has significant oversight responsibilities regarding directing, evaluating, and monitoring of controls. The board's oversight role should encompass aspects of IT governance such as - Organization and governance structures. - Executive leadership and support. - Strategic and operational planning. - Service delivery and measurement. - IT organization and risk management.

Principle 12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
• Establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions. • Establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside. • Assures that competent personnel with sufficient authority perform control activities with diligence and continuing focus, in a timely manner as defined by policies and procedures. • Assures that responsible personnel investigate and act on matters identified as a result of executing control activities. • Periodically reviews control activities to determine their continued relevance, and refreshes them when necessary.	• Monitors compliance with specific policies and procedures as designated by management. • Assists management in the development and communication of policies and procedures. • Ensures that risks are monitored in relation to the organization's established risk appetite.	• Provides assurance regarding the design and implementation of policies, procedures and other controls. • Makes recommendations regarding policies and procedures but normally does not have authority to design or implement policies and procedures for operations residing outside the internal audit function.	• The board provides oversight to ensure that a robust system of policies and procedures is in place to guide operations and helps ensure the accomplishment of objectives.

Principle 13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.			
1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
• Creates and maintains data to monitor day-to-day activities, sharing information across, up, and down the organization. • Considers costs and benefits, ensuring that the nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives. • Information reliability and integrity is a management responsibility. This responsibility includes all critical information of the organization regardless of how the information is stored. Information reliability and integrity includes accuracy, completeness and security.	• Compiles information from across the organization for use in monitoring activities.	• Provides assurance regarding information reliability and integrity and associated risk exposures. This includes both internal and external risk exposures, and exposures relating to the organization's relationships with outside entities. • Periodically assesses the organization's information reliability and integrity practices and recommend as appropriate, enhancements to, or implementation of, new controls and safeguards. Such assessments can either be conducted as separate stand-alone engagements or integrated into other audits or engagements conducted as part of the internal audit plan. • Determines whether or not information reliability and integrity breaches and conditions that might represent a threat to the organization will promptly be made known to senior management, the board and the internal audit activity.	• Senior management and the board leverage information to make decisions to monitor the success of the organization, anticipate risks, and communicate with external stakeholders such as investors. • Periodically receive reports on the operations and effectiveness of the organization's system of internal control.

Principle 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
• Develops and maintains processes for communicating required information to enable all personnel to understand and carry out their internal control responsibilities. • Communicates adequate information to the board of directors to enable them to fulfill their roles with respect to the entity's objectives. • Establishes separate communication channels such as whistleblower hotlines, which serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	• Monitors, compiles information, and communicates summary information to 1st line and 3rd line of defense and the board regarding specific controls. • May be responsible for monitoring separate communication channels such as whistleblower hotlines.	• Provides assurance regarding the completeness, accuracy, and quality of communication in alignment with board and senior management needs.	• The board establishes and communicates the tone it expects across the organization. • The board and senior management should provide guidance regarding the nature of communications expected from individuals in each line of defense.

Principle 15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
• Ensures processes are in place to communicate relevant and timely information to external parties including shareholders, partners, owners, regulators, customers, and financial analysts and other external parties. • Establishes and ensures open communication channels to allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information. • Communicates relevant information from assessments conducted by external parties to the board of directors. • Selects relevant methods of communication and assures that the method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations. • Establishes appropriate policies to address factors such as authorization required for reporting information outside the organization; guidelines regarding permissible and non-permissible information that may be reported; outside persons authorized to receive information and the types of information they may receive; related privacy regulations, regulatory requirements, and legal considerations for reporting information outside the organization; and the nature of assurances, advice, recommendations, opinions, guidance, and other information that may be included in communicating information outside the organization.	• With the exception of certain communications to regulators, external auditors, and other specific groups, normally the second line of defense does not communicate with external parties regarding matters affecting the functioning of internal control. • If the organization reports externally on its internal controls, the second line of defense functions provide management with the results of their activities in support of management's opinions.	• Provides assurance that the essential communications of others are accurate. • Normally the internal audit function does not communicate with external parties regarding matters affecting the functioning of internal control.	• The board should receive information and reports from management on the functioning and effectiveness of internal control and the basis for management's opinions prior to communications with external parties. • The board should discuss with the external auditors their views and opinions that would be included in any external reporting on the organization's control systems.

Principle 16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

1st Line of Defense (Risk Owners/ Managers)	2nd Line of Defense (Risk, Control, and Compliance)	3rd Line of Defense (Internal Auditing)	Other
• Selects and develops a balance of ongoing and separate evaluations, considering the rate of change in business and business processes, and varying the scope and frequency of separate evaluations depending on risk. (These evaluations may be performed by the 2nd line of defense.) • Ensures that evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated. • The design and current state of the internal control system can be used to establish a baseline for ongoing and separate evaluations. • Reports periodically to the board on the performance of the organization's risk management activities.	• Performs ongoing and separate evaluations to monitor the status of various components of the system of internal control as directed by management. • Performs ongoing and separate evaluations to monitor whether achievement of objectives is within established risk tolerances.	• Provides assurance that ongoing management evaluations are built into business processes and adjusted to changing conditions as appropriate. • Provides assurance that information provided by management evaluations is fair and accurately presented. • Provides assurance that the system of internal control is operating as expected and risks are managed within the organization's risk appetite and tolerance.	• The board provides oversight and holds management accountable for selecting, developing, and performing evaluations of the components of internal control. • Receives periodic reports on the organization's risk and effectiveness of its risk management activities.

Principle 17. 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.			
1st Line of Defense (Risk Owners/ Managers)	**2nd Line of Defense** (Risk, Control, and Compliance)	**3rd Line of Defense** (Internal Auditing)	**Other**
• Communicates information about deficiencies to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate. • Tracks whether deficiencies are remediated on a timely basis.	• Individuals in the second line of defense may be delegated responsibility for monitoring and reporting regarding specific types of control deficiencies.	• Internal auditors establish and maintain a system to monitor the disposition of internal audit findings and recommendations communicated to management. This system normally addresses: - The time frame within which management's response to the engagement observations and recommendations is required. - Evaluation of management's response. - Verification of the response (if appropriate). - Performance of a follow-up engagement (if appropriate). - A communications process that escalates unsatisfactory responses/actions, including the assumption of risk, to the appropriate levels of senior management or the board.	• The board should ensure that it receives information regarding control deficiencies in a timely manner and that corrective actions are timely and sufficient to address significant control deficiencies. • Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.

About the Authors

Douglas J. Anderson, CIA, CPA, CRMA, CMA, is Chief Audit Executive Subject Matter Consultant for The IIA's Audit Executive Center®, an Executive-in-Residence at Saginaw Valley State University, and provides consulting services focusing on governance, risk, and control. Anderson has more than 30 years of experience in internal auditing, external auditing, accounting, and finance. His job responsibilities have taken him throughout the world and provided him experience with a wide variety of organizations. Anderson has held a number of volunteer roles with The Institute of Internal Auditors including instructor, member/chair of the Professional Guidance Committee and vice chair of Professional Guidance on the Executive Committee of the Board of Directors. He also served on the Standing Advisory Group of the Public Company Accounting Oversight Board and has been a member of oversight groups for two COSO projects.

Gina Eubanks, CIA, CISA, CRMA, CCSA, is the vice president of Professional Services at The IIA, where she leads the Quality, Chief Audit Executive, and Industry Services programs. She has more than 20 years of experience in internal auditing, including 15 years with a Big 4 firm in global enterprise risk services. Eubanks' experience has been both within the United States and abroad, having spent significant time in India. She has also been a practitioner and director in the retail and financial services sectors. Eubanks also is a member of the audit committee of a local financial institution and was a volunteer leader with The IIA for almost 15 years.

About COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

About The IIA

The Institute of Internal Auditors (The IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 180,000 members from 170 countries. The association's global headquarters are in Altamonte Springs, Fla. For more information, visit theiia.org.

The Institute of Internal Auditors' Audit Executive Center® is the essential resource to empower CAEs to be more successful. The Center's suite of information, products, and services enables CAEs to respond to the unique challenges and emerging risks of the profession. For more information on the Center, visit theiia.org/cae.

This publication contains general information only and none of COSO, any of its constituent organizations or any of the authors of this publication is, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. Information contained herein is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Views, opinions or interpretations expressed herein may differ from those of relevant regulators, self-regulatory organizations or other authorities and may reflect laws, regulations or practices that are subject to change over time.

Evaluation of the information contained herein is the sole responsibility of the user. Before making any decision or taking any action that may affect your business with respect to the matters described herein, you should consult with relevant qualified professional advisors. COSO, its constituent organizations and the authors expressly disclaim any liability for any error, omission or inaccuracy contained herein or any loss sustained by any person who relies on this publication.

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C103046