IIA Position Paper:

THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL

JANUARY 2013

TABLE OF CONTENTS

IIA POSITION PAPER:

THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL

INTRODUCTION

In twenty-first century businesses, it's not uncommon to find diverse teams of internal auditors, enterprise risk management specialists, compliance officers, internal control specialists, quality inspectors, fraud investigators, and other risk and control professionals working together to help their organizations manage risk. Each of these specialties has a unique perspective and specific skills that can be invaluable to the organizations they serve, but because duties related to risk management and control are increasingly being split across multiple departments and divisions, duties must be coordinated carefully to assure that risk and control processes operate as intended.

It's not enough that the various risk and control functions exist — the challenge is to assign specific roles and to coordinate effectively and efficiently among these groups so that there are neither "gaps" in controls nor unnecessary duplications of coverage. Clear responsibilities must be defined so that each group of risk and control professionals understands the boundaries of their responsibilities and how their positions fit into the organization's overall risk and control structure.

The stakes are high. Without a cohesive, coordinated approach, limited risk and control resources may not be deployed effectively, and significant risks may not be identified or managed appropriately. In the worst cases, communications among the various risk and control groups may devolve to little more than an ongoing debate about whose job it is to accomplish specific tasks.

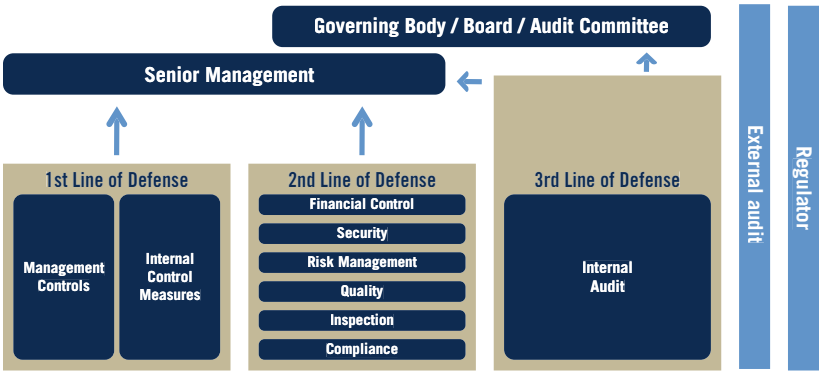
The problem can exist at any organization, regardless of whether a formal enterprise risk management framework is used. Although risk management frameworks can effectively identify the types of risks that modern businesses must control, these frameworks are largely silent about how specific duties should be assigned and coordinated within the organization.

Fortunately, best practices are emerging that can help organizations delegate and coordinate essential risk management duties with a systematic approach. The Three Lines of Defense model provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties. It provides a fresh look at operations, helping to assure the ongoing success of risk management initiatives, and it is appropriate for any organization — regardless of size or complexity. Even in organizations where a formal risk management framework or system does not exist, the Three Lines of Defense model can enhance clarity regarding risks and controls and help improve the effectiveness of risk management systems.

BEFORE THE THREE LINES: RISK MANAGEMENT OVERSIGHT AND STRATEGY-SETTING

In the Three Lines of Defense model, management control is the first line of defense in risk management, the various risk control and compliance oversight functions established by management are the second line of defense, and independent assurance is the third. Each of these three "lines" plays a distinct role within the organization's wider governance framework.

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Although neither governing bodies nor senior management are considered to be among the three "lines" in this model, no discussion of risk management systems could be complete without first considering the essential roles of both governing bodies (i.e., boards of directors or equivalent bodies) and senior management. Governing bodies and senior management are the primary stakeholders served by the "lines," and they are the parties best positioned to help ensure that the Three Lines of Defense model is reflected in the organization's risk management and control processes.

Senior management and governing bodies collectively have responsibility and accountability for setting the organization's objectives, defining strategies to achieve those objectives, and establishing governance structures and processes to best manage the risks in accomplishing those objectives. The Three Lines of Defense model is best implemented with the active support and guidance of the organization's governing body and senior management.

THE FIRST LINE OF DEFENSE: OPERATIONAL MANAGEMENT

The Three Lines of Defense model distinguishes among three groups (or lines) involved in effective risk management:

- **Functions that own and manage risks.**
- **Functions that oversee risks.**
- **Functions that provide independent assurance.**

As the first line of defense, operational managers own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies.

Operational management is responsible for maintaining 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 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.

Operational management naturally serves as the first line of defense because controls are designed into systems and processes under their guidance of operational management. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events.

THE SECOND LINE OF DEFENSE: RISK MANAGEMENT AND COMPLIANCE FUNCTIONS

In a perfect world, perhaps only one line of defense would be needed to assure effective risk management. In the real world, however, a single line of defense often can prove inadequate. Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-defense controls. The specific functions will vary by organization and industry, but typical functions in this second line of defense include:

- A risk management function (and/or committee) that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.
- A compliance function to monitor various specific risks such as noncompliance with applicable laws and regulations. In this capacity, the separate function reports directly to senior management, and in some business sectors, directly to the governing body. Multiple compliance functions often exist in a single organization, with responsibility for specific types of compliance monitoring, such as health and safety, supply chain, environmental, or quality monitoring.
- A controllership function that monitors financial risks and financial reporting issues.

Management establishes these functions to ensure the first line of defense is properly designed, in place, and operating as intended. Each of these functions has some degree of independence from the first line of defense, but they are by nature management functions. As management functions, they may intervene directly in modifying and developing the internal control and risk systems. Therefore, the second line of defense serves a vital purpose but cannot offer truly independent analyses to governing bodies regarding risk management and internal controls.

The responsibilities of these functions vary on their specific nature, but can include:

- **Supporting management policies, defining roles and responsibilities, and setting goals for implementation.**
- **Providing risk management frameworks.**
- **Identifying known and emerging issues.**
- **Identifying shifts in the organization's implicit risk appetite.**
- **Assisting management in developing processes and controls to manage risks and issues.**

- **Providing guidance and training on risk management processes.**
- **Facilitating and monitoring implementation of effective risk management practices by operational management.**
- **Alerting operational management to emerging issues and changing regulatory and risk scenarios.**
- **Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.**

THE THIRD LINE OF DEFENSE: INTERNAL AUDIT

Internal auditors provide the governing body and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organization. This high level of independence is not available in the second line of defense. Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives. The scope of this assurance, which is reported to senior management and to the governing body, usually covers:

- A broad range of objectives, including efficiency and effectiveness of operations; safeguarding of assets; reliability and integrity of reporting processes; and compliance with laws, regulations, policies, procedures, and contracts.
- All elements of the risk management and internal control framework, which includes: internal control environment; all elements of an organization's risk management framework (i.e., risk identification, risk assessment, and response); information and communication; and monitoring.
- The overall entity, divisions, subsidiaries, operating units, and functions — including business processes, such as sales, production, marketing, safety, customer functions, and operations — as well as supporting functions (e.g., revenue and expenditure accounting, human resources, purchasing, payroll, budgeting, infrastructure and asset management, inventory, and information technology).

Establishing a professional internal audit activity should be a governance requirement for all organizations. This is not only important for larger and medium-sized organizations but also may be equally important for smaller entities, as they may face equally complex environments with a less formal, robust organizational structure to ensure the effectiveness of its governance and risk management processes.

Establishing a professional internal audit activity should be a governance requirement for all organizations. This is not only important for larger and medium-sized organizations but also may be equally important for smaller entities, as they may face equally complex environments with a less formal, robust organizational structure to ensure the effectiveness of its governance and risk management processes.

Internal audit actively contributes to effective organizational governance providing certain conditions — fostering its independence and professionalism — are met. Best practice is to establish and maintain an independent, adequately, and competently staffed internal audit function, which includes:

- **Acting in accordance with recognized international standards for the practice of internal auditing.**
- **Reporting to a sufficiently high level in the organization to be able to perform its duties independently.**
- **Having an active and effective reporting line to the governing body.**

EXTERNAL AUDITORS, REGULATORS, AND OTHER EXTERNAL BODIES

External auditors, regulators, and other external bodies reside outside the organization's structure, but they can have an important role in the organization's overall governance and control structure. This is particularly the case in regulated industries, such as financial services or insurance. Regulators sometimes set requirements intended to strengthen the controls in an organization and on other occasions perform an independent and objective function to assess the whole or some part of the first, second, or third line of defense with regard to those requirements. When coordinated effectively, external auditors, regulators, and other groups outside the organization can be considered as additional lines of defense, providing assurance to the organization's shareholders, including the governing body and senior management.
Given the specific scope and objectives of their missions, however, the risk information gathered is generally less extensive than the scope addressed by an organization's internal three lines of defense.

COORDINATING THE THREE LINES OF DEFENSE

Because every organization is unique and specific situations vary, there is no one "right" way to coordinate the Three Lines of Defense. When assigning specific duties and coordinating among risk management functions, however, it can be helpful to keep in mind the underlying role of each group in the risk management process.

FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk Owners/Managers	**Risk Control and Compliance**	**Risk Assurance**
• operating management	• limited independence • reports primarily to management	• internal audit • greater independence • reports to governing body

All three lines should exist in some form at every organization, regardless of size or complexity. Risk management normally is strongest when there are three separate and clearly identified lines of defense. However, in exceptional situations that develop, especially in small organizations, certain lines of defense may be combined. For example, there are instances where internal audit has been requested to establish and/or manage the organization's risk management or compliance activities. In these situations, internal audit should communicate clearly to the governing body and senior management the impact of the combination. If dual responsibilities are assigned to a single person or department, it would be appropriate to consider separating the responsibility for these functions at a later time to establish the three lines.

Regardless of how the Three Lines of Defense model is implemented, senior management and governing bodies should clearly communicate the expectation that information be shared and activities coordinated among each of the groups responsible for managing the organization's risks and controls. Under the *International Standards for the Professional Practice of Internal Auditing*, 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."

RECOMMENDED PRACTICES:

- Risk and control processes should be structured in accordance with the Three Lines of Defense model.
- Each line of defense should be supported by appropriate policies and role definitions.
- There should be proper coordination among the separate lines of defense to foster efficiency and effectiveness.
- Risk and control functions operating at the different lines should appropriately share knowledge and information to assist all functions in better accomplishing their roles in an efficient manner.
- Lines of defense should not be combined or coordinated in a manner that compromises their effectiveness.
- In situations where functions at different lines are combined, the governing body should be advised of the structure and its impact. For organizations that have not established an internal audit activity, management and/or the governing body should be required to explain and disclose to their stakeholders that they have considered how adequate assurance on the effectiveness of the organization's governance, risk management, and control structure will be obtained.

All three lines should exist in some form at every organization, regardless of size or complexity. Risk management normally is strongest when there are three separate and clearly identified lines of defense.

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit acknowledged leader, chief advocate, and principal educator.

Position Papers

Position Papers are part of The IIA's International Professional Practices Framework (IPPF), the conceptual framework that organizes authoritative guidance promulgated by The IIA. A trustworthy, global, guidance-setting body, The IIA provides internal audit professionals worldwide with authoritative guidance organized in the IPPF as mandatory guidance and strongly recommended guidance. Position papers are part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes.

Position Papers assist a wide range of interested parties, including those not in the internal audit profession, in understanding significant governance, risk, or control issues, and delineating the related roles and responsibilities of internal auditing.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance.

Disclaimer

Copyright

The Institute of Internal Auditors Global

Global Headquarters
247 Maitland Avenue
Altamonte Springs, Florida 32701 USA

T +1-407-937-1111
F +1-407-937-1101
W www.globaliia.org

12691-2