POSITION PAPER

# The IIA's Three Lines Model

## An Update of the Three Lines of Defense

The Institute of Internal Auditors

# Contents

# Introduction

**Organizations are human** undertakings operating in an increasingly uncertain, complex, interconnected, and volatile world. They often have multiple stakeholders with diverse, changeable, and sometimes competing interests. Stakeholders entrust organizational oversight to a governing body, which in turn delegates resources and authority to management to take appropriate actions, including managing risk.

For these reasons and more, organizations need effective structures and processes to enable the achievement of objectives while supporting strong governance and risk management. As the governing body receives reports from management on activities, outcomes, and forecasts, both the governing body and management rely on the internal audit function to provide independent, objective assurance and advisory services on all matters and to promote and facilitate innovation and improvement. The governing body is ultimately accountable for governance, which is achieved through the actions and behaviors of the governing body as well as management and internal audit.

The Three Lines Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management.

## Key terms

- organization – An organized group of activities, resources, and people working toward shared goals.
- stakeholder* – A party with a direct or indirect interest in an organization's activities and outcomes. Stakeholders may include the board, management, employees, customers, vendors, shareholders, regulatory agencies, financial institutions, external auditors, the public, and others.
- governing body – The highest-level body charged with governance, termed "board" in the Global Internal Audit Standards™. In an organization that has more than one governing body, board refers to the body/bodies authorized to provide the internal audit function with the appropriate authority, role, and responsibilities.
- management – Those individuals, teams, and support functions assigned to provide products and/or services to the organization's clients.
- internal auditing* – An independent, objective assurance and advisory service 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 governance, risk management, and control processes.
- internal audit function* – A professional individual or group responsible for providing an organization with assurance and advisory services.
- control* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

*Terms with asterisks come from the Global Internal Audit Standards™ glossary.

The model applies to all organizations and is optimized by:

- Adopting a principles-based approach and adapting the model to suit organizational objectives and circumstances.
- Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of “defense” and protecting value.
- Clearly understanding the roles and responsibilities represented in the model and the relationships among them.
- Implementing measures to ensure activities and objectives are aligned with the prioritized interests of stakeholders.

# Principles of the Three Lines Model

## Principle 1: Governance

**The governance of an** organization requires appropriate structures and processes that enable:

- Accountability by a governing body to stakeholders for organizational oversight through integrity, leadership, and transparency.
- Actions (including managing risk) by management to achieve the objectives of the organization through risk-based decision-making and application of resources.
- Assurance and advice by an independent internal audit function to provide clarity and confidence and to promote and facilitate continuous improvement through rigorous inquiry and insightful communication.

## Principle 2: Governing body roles

The governing body ensures:

- Appropriate structures and processes are in place for effective governance.
- Organizational objectives and activities are aligned with the prioritized interests of stakeholders.

### Key terms

- risk-based decision-making – A considered process that includes analysis, planning, action, monitoring, and review, and takes account of potential impacts of uncertainty on objectives.
- assurance* – Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, and control processes over an issue, condition, subject matter, or activity under review when compared to established criteria.
- governance* – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.
- advisory services* – Services through which internal auditors provide advice to an organization's stakeholders without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. Examples include advising on the design and implementation of new policies, processes, systems, and products; providing forensic services; providing training; and facilitating discussions about risks and controls. "Advisory services" are also known as "consulting services."
- assurance services* – Services through which internal auditors perform objective assessments to provide assurance. Examples of assurance services include compliance, financial, operational/performance, and technology engagements. Internal auditors may provide limited or reasonable assurance, depending on the nature, timing, and extent of procedures performed.

*Terms with asterisks come from the Global Internal Audit Standards™ glossary.

The governing body:

- Delegates responsibility and provides resources to management to achieve the objectives of the organization while ensuring legal, regulatory, and ethical expectations are met.
- Establishes and oversees an independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of objectives.

## Principle 3: Management and first and second line roles

Management's responsibility to achieve organizational objectives comprises both first and second line roles.[1] First line roles are most directly aligned with the delivery of products and/or services to clients of the organization and include the roles of support functions[2]. Second line roles assist with managing risk.

First and second line roles may be blended or separated. Some second line roles may be assigned to specialists to provide complementary expertise, support, monitoring, and challenge to those with first line roles. Second line roles can focus on specific objectives of risk management, such as: compliance with laws, regulations, and acceptable ethical behavior; controls; information and technology security; sustainability; and quality assurance. Alternatively, second line roles may span a broader responsibility for risk management, such as enterprise risk management (ERM). However, responsibility for managing risk remains a part of first line roles and within the scope of management.

## Principle 4: Third line roles

The internal audit function provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.[3] It achieves this through the competent application of systematic and disciplined processes, expertise, and insight. It reports its findings to management and the governing body to promote and facilitate continuous improvement. In doing so, it may consider assurance from other internal and external providers.

## Principle 5: Third line independence

Internal audit's independence from the responsibilities of management is critical to its objectivity, authority, and credibility. It is established through accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of audit services.

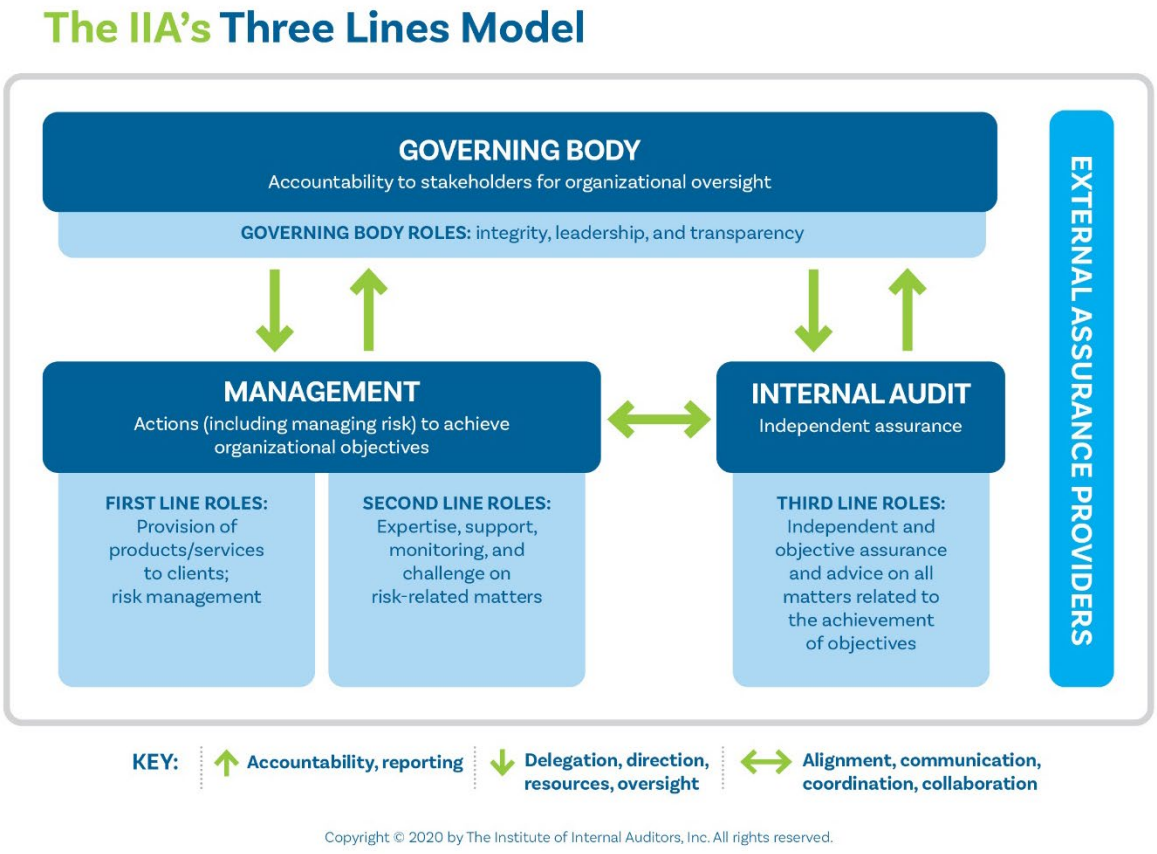
1. The language of "first line," "second line," and "third line" is retained from the original model in the interests of familiarity. However, the "lines" are not intended to denote structural elements but a useful differentiation in roles. Logically, governing body roles also constitute a "line" but this convention has not been adopted to avoid confusion. The numbering (first, second, third) should not be taken to imply sequential operations. Instead, all roles operate concurrently.

2. Some consider the roles of support functions (such as HR, administration, and building services) to be second line roles. For clarity, the Three Lines Model regards first line roles to include both "front of house" and "back office" activities, and second line roles to comprise those complementary activities focused on risk-related matters.

3. In some organizations, other third line roles are identified, such as oversight, inspection, investigation, evaluation, and remediation, which may be part of the internal audit function or operate separately.

## Principle 6: Creating and protecting value

All roles working together collectively contribute to the creation and protection of value when they are aligned with each other and with the prioritized interests of stakeholders. Alignment of activities is achieved through communication, cooperation, and collaboration. This ensures the reliability, coherence, and transparency of information needed for risk-based decision-making.



# Key Roles in the Three Lines Model

**Organizations differ considerably** in their distribution of responsibilities. However, the following high-level roles serve to amplify the Principles of the Three Lines Model.

## Governing body

- Accepts accountability to stakeholders for oversight of the organization.
- Engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives.
- Nurtures a culture promoting ethical behavior and accountability.
- Establishes structures and processes for governance, including auxiliary committees as required.
- Delegates responsibility and provides resources to management for achieving the objectives of the organization.
- Determines organizational appetite for risk and exercises oversight of risk management (including controls).
- Maintains oversight of compliance with legal, regulatory, and ethical expectations.
- Establishes and oversees an independent, objective, and competent internal audit function.

## Management

### *First line roles*

- Leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organization.
- Maintains a continuous dialogue with the governing body, and reports on planned, actual, and expected outcomes linked to the objectives of the organization; and risk.
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including controls).
- Ensures compliance with legal, regulatory, and ethical expectations.

### *Second line roles*

- Provides complementary expertise, support, monitoring, and challenge related to the management of risk, including:
    - The development, implementation, and continuous improvement of risk management practices (including controls) at a process, systems, and entity level.
    - The achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behavior; controls; information and technology security; sustainability; and quality assurance.
- Provides analysis and reports on the adequacy and effectiveness of risk management (including controls).

## Internal audit function

- Maintains primary accountability to the governing body and independence from the responsibilities of management.
- Communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management (including controls) to support the achievement of organizational objectives and to promote and facilitate continuous improvement.
- Reports impairments to independence and objectivity to the governing body and implements safeguards as required.

## External assurance providers

- Provide additional assurance to:
  - Satisfy legislative and regulatory expectations that serve to protect the interests of stakeholders.
  - Satisfy requests by management and the governing body to complement internal sources of assurance.

# Relationships Among Core Roles

## Between the governing body and management (both first and second line roles)

**The governing body typically** sets the direction of the organization by defining the vision, mission, values, and organizational appetite for risk. It then delegates responsibility for the achievement of the organization's objectives to management, along with the necessary resources. The governing body receives reports from management on planned, actual, and expected outcomes, as well as reports on risk and the management of risk.

### Key term

chief executive officer (CEO) – The most senior individual in the organization with responsibility over operations.

Organizations vary as to the degree of overlap and separation between the roles of the governing body and management. The governing body can be more or less "hands on" with respect to strategic and operational matters. Either the governing body or management may take the lead in developing the strategic plan, or it may be a shared undertaking. In some jurisdictions, the CEO may be a member of the governing body and may even be its chair. In all cases, there needs to be strong communication between management and the governing body. The CEO is typically the focal point for this communication, but other senior managers may have frequent interactions with the governing body. Organizations may wish, and their regulators may require, leaders of second line roles such as a chief risk officer and a chief compliance officer to have a direct reporting line to the governing body. This is fully consistent with the Principles of the Three Lines Model.

## Between management (both first and second line roles) and the internal audit function

Internal audit's independence from management ensures it is free from hindrance and bias in its planning and in the carrying out of its work, enjoying unfettered access to the people, resources, and information it requires. It is accountable to the governing body. However, independence does not imply isolation. There must be regular interaction between the internal audit function and management to ensure internal audit work is relevant and aligned with the strategic and operational needs of the organization. Through all its activities, the internal audit function builds its knowledge and understanding of the organization, which contributes to the assurance and advisory services it delivers as a trusted advisor and strategic partner. There is a need for collaboration and communication across both the first and second line roles of management and the internal audit function to ensure there is no unnecessary duplication, overlap, or gaps.

## Between the internal audit function and the governing body

The internal audit function is accountable to, and sometimes described as being the "eyes and ears" of, the governing body.

The governing body is responsible for oversight of internal audit, which requires: ensuring an independent internal audit function is established, including the hiring and firing of the chief audit executive; serving as the primary reporting line for the CAE;[4] approving and resourcing the audit plan; receiving and considering reports from the CAE; and enabling free access by the CAE to the governing body, including private sessions without the presence of management.

### Key term

chief audit executive (CAE)* – The leadership role responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services in accordance with Global Internal Audit Standards. The specific job title and/or responsibilities may vary across organizations.

*Terms with asterisks come from the Global Internal Audit Standards™ glossary

## Among all roles

The governing body, management, and the internal audit function have their distinct responsibilities, but all activities need to be aligned with the objectives of the organization. The basis for successful coherence is regular and effective coordination, collaboration, and communication.

4. For administrative purposes, the CAE may also report to an appropriately senior level of management.

# Applying the Model

## Structure, roles, and responsibilities

**The Three Lines Model is most effective** when it is adapted to align with the objectives and circumstances of the organization. How an organization is structured and how roles are assigned are matters for management and the governing body to determine. The governing body may establish committees to provide additional oversight for particular aspects of its responsibility, such as audit, risk, finance, planning, and compensation. Within management, there are likely to be functional and hierarchical arrangements and an increasing tendency toward specialization as organizations grow in size and complexity.

Functions, teams, and even individuals may have responsibilities that include both first and second line roles. However, direction and oversight of second line roles may be designed to secure a degree of independence from those with first line roles — and even from the most senior levels of management — by establishing primary accountability and reporting lines to the governing body. The Three Lines Model allows for as many reporting lines between management and the governing body as required. In some organizations, most notably regulated financial institutions, there is a statutory requirement for such arrangements to ensure sufficient independence. Even in these situations, those in management with first line roles remain responsible for managing risk.

Second line roles may include monitoring, advice, guidance, testing, analyzing, and reporting on matters related to the management of risk. Insofar as these provide support and challenge to those with first line roles and are integral to management decisions and actions, second line roles are part of management's responsibilities and are never fully independent from management, regardless of reporting lines and accountabilities.

A defining characteristic of third line roles is independence from management. The Principles of the Three Lines Model describe the importance and nature of internal audit independence, setting the internal audit function apart from other functions and enabling the distinctive value of its assurance and advisory services. The internal audit function's independence is safeguarded by not making decisions or taking actions that are part of management's responsibilities (including risk management) and by declining to provide assurance on activities for which the function has current, or has had recent, responsibility. For example, in some organizations, the CAE is asked to assume additional decision-making responsibilities over activities utilizing similar competencies, such as aspects of statutory compliance or ERM. In such circumstances, the internal audit function is not independent of these activities or of their results, and therefore, when the governing body seeks independent and objective assurance and advice relating to those areas, it is necessary for its provision to be undertaken by a qualified third party.

## Oversight and assurance

The governing body relies on reports from management (comprising those with first and second line roles), internal audit, and others in order to exercise oversight and achievement of its objectives, for which it is accountable to stakeholders. Management provides valuable assurance (also referred to as attestations) on planned, actual, and forecast outcomes, on risk, and on risk management by drawing upon direct experience and expertise. Those with second line roles provide additional assurance on risk-related matters. Because of internal audit's independence from management, the assurance it provides carries the highest degree of objectivity and confidence beyond that which those with first and second line roles can provide to the governing body, irrespective of reporting lines. Further assurance may also be drawn from external providers.

## Coordination and alignment

Effective governance requires appropriate assignment of responsibilities as well as strong alignment of activities through cooperation, collaboration, and communication. The governing body seeks confirmation through the internal audit function that governance structures and processes are appropriately designed and operating as intended.

## About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 245,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance.

For more information, visit theiia.org.

## Disclaimer



## Copyright



Updated September 2024

The Institute of
Internal Auditors

**Global Headquarters**
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101