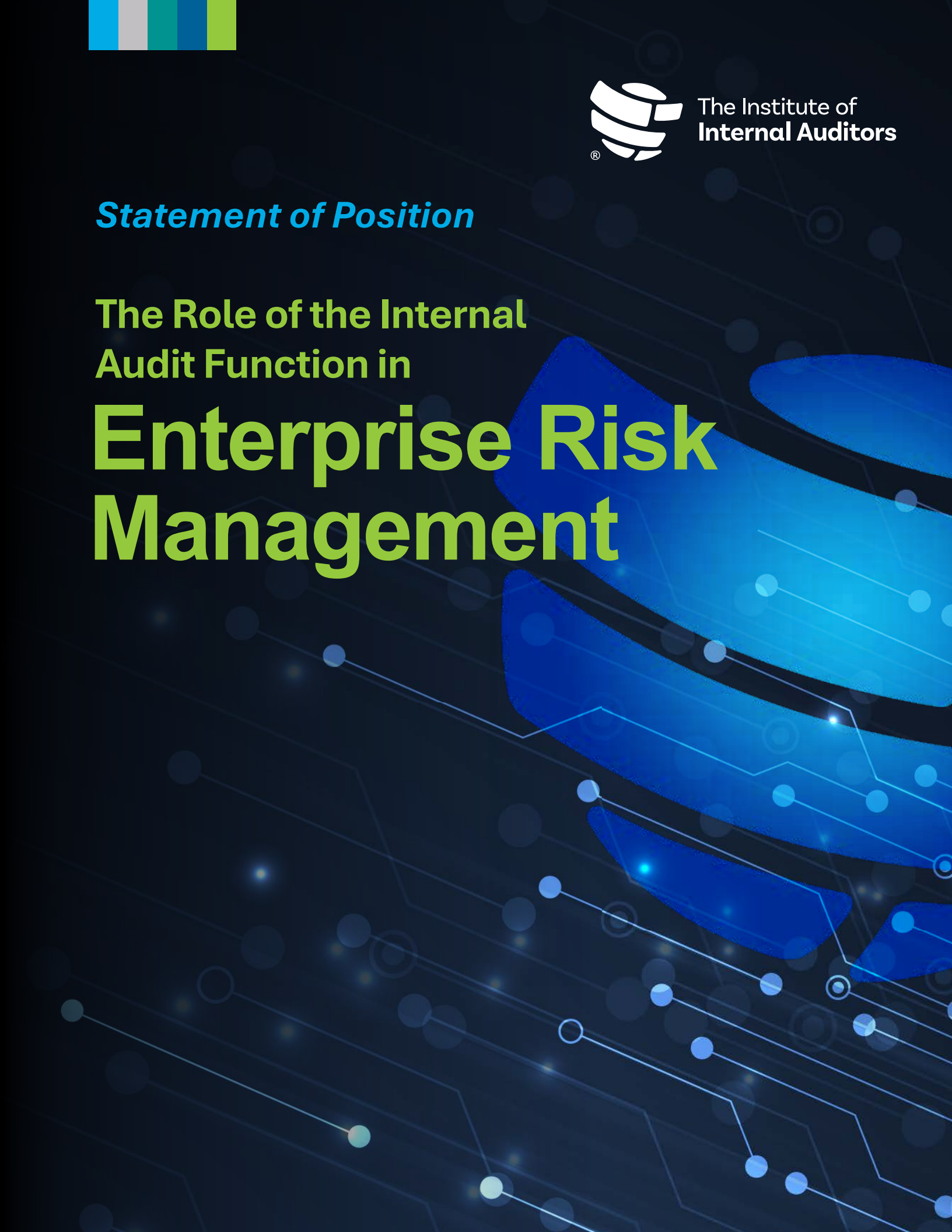
The Institute of Internal Auditors

Statement of Position

The Role of the Internal Audit Function in Enterprise Risk Management



Contents

Executive Summary

This Statement of Position clarifies the role of the internal audit function in Enterprise risk management (ERM). Organizations require effective governance, risk management, compliance, and control processes to achieve objectives and sustain long-term value. ERM provides a coordinated, organizationwide approach to identifying, assessing, managing, monitoring, and reporting threats and opportunities, enabling resilience and alignment with strategic objectives. In increasingly data-driven environments, effective ERM supports reliable decision-making by the board and management.

ERM operates within a governance framework characterized by distinct accountabilities:

- The board establishes expectations and oversees senior management.
- Management is responsible for managing risks and implementing ERM processes.
- The internal audit function provides independent, risk-based, and objective assurance, advice, insight, and foresight. Independence and objectivity are fundamental to the credibility of the internal audit function.

The internal audit function strengthens ERM by providing assurance and advisory services that are complementary and mutually reinforcing:

- Assurance: Assesses the design and effectiveness of ERM processes, including their alignment with risk appetite, risk tolerance, strategy, and governance expectations.
- Advisory: Provides insights and foresight to strengthen ERM practices, including challenging assumptions, facilitating risk discussions, and sharing good practices, without assuming management responsibility.

The balance between assurance and advisory services is determined by organizational context, including ERM maturity, the risk environment, the capability of other functions, and direction from the board. As governance and management structures evolve to meet changing organizational needs and future objectives, these services are enhanced when coordinated or integrated with other assurance and advisory providers across the organization. The internal audit function supports integrated assurance by promoting alignment, reducing duplication, and enabling a coherent view of governance, risk management, compliance, and control effectiveness for the board and senior management.

Some organizations assign responsibility for ERM activities to the chief audit executive, due to organizational maturity, resource constraints, relevant skills, or other factors. However, when the chief audit executive takes on responsibility for ERM activities, safeguards must ensure that:

- Responsibilities are clearly defined and documented.
- Assurance and advisory roles are appropriately separated.
- Potential impairments are transparent to the board.
- Independent assurance is obtained where the internal audit function has operational involvement.
- The internal audit function does not assume responsibility for risk management decisions.

Part I – Principles-Based Framework

Purpose and Context

Organizations require effective governance, risk management, compliance, and control structures and processes to achieve their objectives and sustain long-term value. Boards are accountable to stakeholders for governing the organization. This requires reliable, balanced information regarding performance, risks, and controls. Senior management is accountable to the board for designing structures and processes to achieve objectives and manage risks.

Enterprise risk management (ERM) activities support these needs by integrating threat and opportunity considerations into strategy, decision-making, and performance. As organizations increasingly rely on data to inform decisions and monitor performance, independent insight and assurance over risk-related information become increasingly important. At the same time, ERM activities help structure and align governance, risk management, compliance, and control processes, enabling accountability, responsibility, and coordination across the organization.

> *This Statement of Position uses the term "board" to refer to various forms of governing bodies and their committees, as described in the Glossary.*

This Statement of Position clarifies the role of the internal audit function in ERM within a modern governance environment. It provides principles-based guidance that emphasizes the importance of independence and objectivity to the internal audit function while recognizing that insight, foresight, coordination, and integration of assurance and ERM activities strengthen governance and risk management processes when appropriately structured. The Statement's underlying principles apply to all organizations, though the implementation of governance, risk management, compliance, and control structures and processes is specific to each organization.

Together with the Statement of Position "Three Lines Model: Assurance and Advice in Support of Effective Governance," The IIA provides a consistent, flexible framework to support organizational governance and ERM roles and responsibilities that meet the needs of the organization and its stakeholders.

Audience

The primary audience for this Statement of Position is chief audit executives and internal auditors who navigate expectations related to ERM. It is also written to be shared with boards, audit and risk committees, chief risk officers, senior executives, regulators, and other assurance and advisory functions as a reference point for how the internal audit function can contribute to ERM without assuming management's responsibility for making strategic or operational decisions.

Defining Enterprise Risk Management

Enterprise risk management (ERM) is a coordinated, organizationwide approach through which risks (threats and opportunities) are identified, assessed, managed, monitored, and reported. ERM supports achievement of strategic objectives, decision-making, sustainable value creation, and resilience within the organization's governance, risk appetite, and cultural context.

This definition reflects a modern view of ERM as a continuous, dynamic set of processes embedded in decision-making and performance, rather than a periodic exercise or a static risk register. It recognizes that ERM is organizationwide and integrated across functions, connecting strategy, operations, finance, compliance, and culture. It also reinforces that risk includes both threats and opportunities and is, therefore, directly linked to how the organization seeks to create, protect, and sustain value.

ERM is scalable and principles-based; it is designed and applied in a way that fits organizational context, maturity, and complexity, while still providing a coherent enterprise-level view that supports board oversight and senior management supervision and decision-making. However, legal and regulatory requirements may preclude certain organizational structures or assignments of responsibilities.

ERM does not replace other day-to-day risk management activities. The management of operational, financial, compliance, technological, and other risks occurs throughout the organization through specific roles and processes that support the design and implementation of control processes to achieve specified objectives. ERM provides the context and integration mechanism that elevates and connects those risk management activities into an organizationwide picture, enabling aggregation, escalation, and informed trade-offs at the executive and board levels. By doing so, ERM helps keep operations within the organization's risk appetite and risk tolerance, ensuring that risk-taking remains aligned with governance expectations and strategic intent.

ERM and Internal Audit Functions Within the Governance System

The board is ultimately accountable to stakeholders for overseeing senior management's approach to risk management. The board establishes the organization's risk appetite and risk tolerance, and ensures that risk-related reporting supports effective oversight and decision-making. Senior management is responsible for establishing structures and processes to achieve objectives and manage risks, including creating second-line functions and roles to provide specialist support, monitoring, and challenge to first-line decisions. ERM activities help ensure that the board and senior management receive timely, decision-useful information about the organization's achievement of objectives and management of risks.

The internal audit function, as the third line, is authorized by the board to provide independent, risk-based, and objective assurance and advisory services. Independence does not imply isolation; effective governance depends on coordinated assurance and advice while maintaining clarity of accountability and responsibility.

The Role of the Internal Audit Function in ERM

The internal audit function contributes to ERM through assurance, advisory, and administrative services, which are essential and mutually reinforcing. Boards, senior management, and other stakeholders increasingly expect internal audit functions to deliver assurance that ERM activities are effective, while also providing insights to strengthen how the organization anticipates and responds to emerging uncertainty. This dual contribution is a strength of the internal audit function when boundaries are clear and safeguards are in place.

Skills and Capabilities

Internal auditors possess competencies that enable assessments of risk management, compliance, and control processes across the organization, making them particularly well-suited to perform or advise on ERM activities. This includes expertise in linking risks to strategies and objectives, understanding how risk appetite and risk tolerance are applied at a process level, identifying the expressions of risk culture, and evaluating how risk information informs decision-making.

Internal auditors can also leverage strengths in data analytics and related technologies to improve the speed and breadth of, and objective support for, ERM activities. Where specialized subject or process expertise is required, the internal audit function should ensure appropriate competence is applied, whether internally or through external support, when undertaking such work.

Internal Audit's Role In Enterprise Risk Management

IIA

INTERNAL AUDIT PROVIDES

Independent Assurance
Provides confidence that ERM processes are designed and operating effectively.

Advisory Insight
Strengthens ERM practices through challenge, facilitation, and sharing of good practices.

Risk-Based Perspective
Uses risk information to prioritize assurance and advisory activities.

Integrated Assurance
Coordinates and aligns assurance perspectives across the organization.

Organizationwide View
Provides a holistic assessment of governance, risk management, compliance, and controls.

COMMON SAFEGUARDS

Clear Responsibilities
Roles are explicitly documented and understood.

Board Approval
Expanded ERM roles are formally approved.

Separation of Assurance & Advice
Assurance is not impaired by advisory work.

Transparency
Potential impairments are disclosed.

External Assurance
Independent assurance is provided over activities internal audit operates.

Assurance Services
Independent and objective assurance over ERM effectiveness.

Advisory Services
Insight and advice to strengthen ERM practices.

Internal Audit Administrative Activities
Activities supporting risk-based audit planning and coordination.

Management Decision-Making
Management ownership of risk decisions and responses. Internal audit must not perform these activities.

ENTERPRISE RISK MANAGEMENT: IDENTIFY • ASSESS • MANAGE • MONITOR • REPORT

Strengthening governance, creating value, and supporting informed decision-making across the ERM lifecycle.

Internal Audit Assurance in Relation to ERM

The internal audit function provides independent and objective assurance to the board and senior management that ERM processes are adequately designed and operating effectively. This includes assurance that risk appetite and risk tolerance are established and embedded into decision-making; threats and opportunities are identified and assessed in a reliable and consistent manner; significant risks are escalated and reported appropriately; and management's responses align with governance expectations.

Assurance over ERM includes evaluating whether it supports strategic objectives and resilience, including how risk information is used in decisions and how risk culture influences incentives and accountability. Because the internal audit function is positioned to take an organizationwide view, it can provide integrated conclusions about the coherence of risk management across the organization, rather than only evaluating isolated components. The internal audit function can also support stronger coordination among assurance providers by contributing to or developing an assurance map, and by helping align perspectives on risk, compliance, and control themes.

When the chief audit executive concludes that management has accepted a level of risk that exceeds the organization's risk appetite or risk tolerance, the matter must be discussed with senior management and escalated to the board as appropriate.

Internal Audit Advice in Relation to ERM

Due to its organizationwide perspective, the internal audit function may also provide advisory services that improve and strengthen ERM activities. Advisory engagements can include facilitating risk workshops and training; advising on the clarity and usability of risk language and methodologies; challenging assumptions and data underlying risk assessment and reporting; and sharing good practices observed across the organization.

Importantly, the internal audit function's advisory contributions do not substitute for first- or second-line management responsibilities. Advisory services should enhance risk management by improving understanding and enabling more informed decisions, while preserving the internal audit function's ability to provide independent assurance. The internal audit function may challenge and advise, but it does not relieve management of responsibility for risk response decisions.

Internal Audit Administrative Activities in Relation to ERM

The internal audit function performs various administrative tasks to fulfill its need for dynamic, risk-based assurance and advice. Such tasks can be associated with the elements of the definition of ERM.

The internal audit plan is based on an assessment of the organization's strategies, objectives, and risks, which are typically represented in a universe of potentially auditable units. The internal audit plan prioritizes engagements based on an assessment of risks aligned with the organization's strategies. Engagement objectives are also based on an assessment of relevant risks. The chief audit executive monitors the organization's performance and emerging risks to align assurance and advisory services with the potential to create, protect, and sustain value. The chief audit executive also consolidates risk reports in collaboration with management and other assurance providers.

Risk Management Functions

Many organizations establish risk management functions to support the implementation, operation, and improvement of ERM processes. Such functions typically perform activities as previously described for the internal audit function and may, in addition:

- Maintain the organization's ERM framework.
- Promulgate risk management policy.
- Provide expert advice on general or subject-specific risk management tools and techniques.
- Monitor specific risks.
- Formulate and report the organization's portfolio view of risk.
- Challenge management decisions and provide thematic reviews in specialist areas.
- Collaborate with the internal audit function to improve the organization's risk management processes.

Risk management roles are categorized as second-line activity in The IIA's Three Lines Model. In some organizations, risk management functions report to the chief audit executive, which necessitates safeguards to protect the independence of the internal audit function.

In organizations that do not have dedicated second-line roles or functions, management may benefit from relying on the internal audit function's processes to identify and provide assurance over significant risks. In such situations, the chief audit executive may help management establish ERM activities as the organization grows and matures.

Whether management has established second-line activities or not, collaboration, coordination, and appropriate reliance among the parties, as well as sufficient safeguards to the internal audit function's independence, contribute to the organization's success.

Internal Audit Function's Involvement Across ERM

ERM activities can be categorized as relating to the following elements of the ERM definition: Identify, Assess, Manage, Monitor, and Report. This activity-based framing helps articulate how internal auditors can collaborate on and contribute to ERM processes without impairing their objectivity or taking on management decision-making responsibilities.

- **Identify**: The internal audit function may advise on risk taxonomy and consistency of language, or even document the linkages between risks and objectives, but should not determine management's approach. The internal audit function's assurance role includes evaluating whether the organization's risk identification is sufficiently complete, consistent with the established taxonomy, and aligned with strategy.
- **Assess**: The internal audit function assesses risks across the organization and within specific processes to prioritize its efforts, and it assesses whether the residual effects of management's risk responses are within the risk appetite and risk tolerance in assurance engagements. The internal audit function may provide general or specialist advice on management's risk assessment methodologies, including scoring and prioritization, and it may challenge assumptions underlying the risk profile. However, it should not be responsible for ongoing risk assessment processes that it later audits. When ERM processes are effective, the internal audit function may place some reliance on management's enterprise risk assessment when prioritizing engagements in the internal audit plan.
- **Manage**: The internal audit function may advise on policies or controls but should not own final policies or risk response decisions. Management must be responsible for policies and decisions and be held accountable by the board. The internal audit function's assurance focuses on whether risk management, compliance, and control processes are effective and efficient.
- **Monitor**: The internal audit function monitors whether action plans to address identified gaps are implemented. It also assesses whether management adequately monitors changes to the organization's risk profile. The internal audit function may advise on incident analyses and key risk indicators, including whether management's monitoring is timely and supports decision-making.
- **Report**: The internal audit function provides assurance over the design and implementation of risk reporting and escalation processes. It may also advise on the clarity and coherence of risk information presented to the board and senior management. Where the internal audit function contributes to integrating risk reporting across lines, it should do so in a way that promotes coherence while maintaining independence.

Safeguards to Preserve Independence and Objectivity

Independence and objectivity are foundational to the internal audit function's credibility. Organizational independence supports internal auditors' ability to maintain objectivity and provide assurance and advice free from undue influence. However, in some organizations, the chief audit executive is responsible for both the internal audit function and a risk management function. When the internal audit function and/or chief audit executive have an expanded role in ERM, safeguards must be deliberate, proportionate, and visible to the board in the internal audit charter. The chief audit executive must not make decisions about or be held accountable for risk responses, as these are management responsibilities and may compromise internal auditors' objectivity.

Effective safeguards typically include:

- **Clear and documented allocation of responsibilities.** Roles across first-line management, second line, and the internal audit function should be explicitly defined at the activity level (for example, who designs risk methodologies, who performs monitoring, who provides assurance). Ambiguity increases the risk of perceived impairment.
- **Formal board approval of expanded responsibilities.** When internal auditors, including the chief audit executive, assume additional ERM-related responsibilities, the board should formally approve the arrangement, for example, in the internal audit charter, and acknowledge the associated risks and mitigation measures. The internal audit function may need the board and senior management to approve additional resources to provide such services with appropriate safeguards.
- **Separation between advisory and assurance work.** When internal auditors provide advisory support (for example, facilitating workshops or advising on ERM enhancements), those engagements should be clearly scoped and documented as advisory services. Subsequent assurance work must be conducted by individuals who were not responsible for designing or operating the processes under review within the last 12 months.
- **Transparent disclosure of potential impairments.** Any actual or perceived threats to objectivity must be communicated to the board. Transparency reinforces trust and enables informed oversight.

- **Ability to challenge ERM responsibilities.**
  The chief audit executive should be able to challenge a proposed assignment of responsibilities that would significantly impair the independence of the internal audit function and must discuss appropriate safeguards with the board. Making the assignment temporary, with a plan to transition the responsibilities to management, may mitigate the potential impacts.
- **Alternative or independent assurance arrangements where necessary.**
  If internal auditors perform or supervise ERM activities, assurance over those areas must be provided by another suitably qualified and independent party, whether internal or external.
- **Periodic external review.**
  In structures where the chief audit executive supervises ERM activities, periodic external quality assessments or targeted independent reviews of the internal audit function can help mitigate perception risks and confirm that independence and objectivity remain intact.

These safeguards enable organizations to adopt structures that suit their context while preserving the credibility of assurance and maintaining the board's confidence in the effectiveness of risk management processes. When safeguards are thoughtfully applied, overlaps in supervision can enhance coordination and insight without compromising independence, objectivity, or accountability.

Coordination and Reliance

Governance, risk management, compliance, and control processes benefit from coordination and appropriate reliance among assurance and advisory providers, internal and external, to the organization. Reliance is appropriate when methodologies and evidence are sufficient and appropriately documented. An assurance map may help identify gaps and duplication. Reliance by the internal audit function on other assurance and advisory providers, and vice versa, should enhance efficiency without transferring accountability or weakening independence and/or objectivity.

The chief audit executive should facilitate an integrated approach to risk assessments and assurance, collaborating with operations and support roles to optimize coverage, reduce redundancies, and enhance insights. The board should maintain visibility over reliance decisions.

Part II – Internal Audit's Role in ERM in Practice

Balancing Assurance and Advice

As both assurance and advisory services are core contributions of the internal audit function, the key question is how to calibrate the right balance in each given context. The mix of services should take into consideration:

- **The maturity and resourcing of ERM.**
  The balance between the internal audit function's assurance and advisory services toward ERM activities may be influenced by the maturity of the organization. Where ERM is evolving or undergoing transformation, advisory support may be more prominent to strengthen frameworks and processes, while preserving the ability to provide independent and objective assurance later. Where ERM activities are well established and embedded, the internal audit function may emphasize providing assurance about effectiveness, reliability, and strategic alignment. However, when ERM activities reach an optimized state, verified by assurance, then advisory services may still be appropriate to enhance contributions to strategy-setting.
- **The organization's strategic and risk context.**
  During periods of rapid change, transformation, or emerging risk, advisory insights can help leadership understand uncertainties and trade-offs. During periods of relative external stability, perhaps with discrete internal incidents or governance concerns, assurance may be favored to reinforce confidence in risk management and reporting.
- **The strength and coordination of other assurance and advisory providers.**
  Where capable second-line functions, such as a risk management function, provide effective monitoring and thematic reviews, the internal audit function may place greater emphasis on coordinated assurance and appropriate reliance, provided such reliance is transparent and does not compromise independence or objectivity.
- **Ongoing direction from and transparency with the board.**
  Significant advisory work should be clearly scoped and documented in alignment with the mandate from the board, and any implications for future assurance should be discussed in advance. When appropriate safeguards are in place, advisory activities can add significant value while preserving the objectivity and credibility required for future assurance engagements.

Scenarios Involving Supervision and Overlapping Responsibilities

In practice, governance and management structures are not always clearly separated. These structures should evolve in response to changing organizational needs and circumstances, guided by a clear vision of the future state and an understanding of practical limitations and potential implications. Organizational size, resource constraints, regulatory expectations, or strategic priorities may result in arrangements where responsibilities relating to ERM overlap with those of the internal audit function. Supervisory overlap is not inherently problematic; what matters is whether activities are assigned to those with relevant skills, management's responsibility for managing risks remains clear, independence and objectivity are preserved for internal auditors, and the board retains confidence in the quality of assurance.

The two scenarios described below are most common, though other organizational structures are possible. They are intended to illustrate common arrangements rather than promote a particular structure, and in some jurisdictions or sectors may not be appropriate due to legal, regulatory, or professional obligations.

Scenario A: The Internal Audit Function Performs Second-Line ERM Activities

In some organizations, particularly smaller or evolving ones, the internal audit function may assume responsibilities typically associated with a risk management function. This may reflect practical necessity, structural design, or a desire to accelerate ERM development. Internal auditors typically possess relevant competencies in identifying, assessing, monitoring, and reporting on risks, compliance, and controls. Such skills can be leveraged to bring structure and integration to the organization's approach to ERM. However, when the internal audit function's responsibilities extend beyond advisory support into operating administrative ERM activities, there are potential impairments to the independence of the internal audit function and the objectivity of the internal auditors, including the chief audit executive.

Viewed across the ERM cycle, this scenario may appear as:

- **Identify:**
  The internal audit function appropriately identifies risks and associates them with organizational objectives for its own audit planning and assurance purposes. The role becomes more extended when management relies on the internal audit function's work and does not develop its own risk taxonomy. The internal audit function may work with management to coordinate organizationwide risk identification processes and develop a shared understanding of significant risks, but management is still responsible for determining appropriate responses.
- **Assess:**
  The internal audit function routinely assesses risks to develop its audit plan and determine engagement priorities. The role broadens when there are no similar, formalized risk assessment activities performed by management, or the internal audit function is asked to develop enterprise risk assessment methodologies, set scoring criteria, maintain an enterprise risk register, or aggregate organizationwide risk ratings.
- **Manage:**
  The internal audit function may appropriately advise on ERM policies or processes, including how to design controls in alignment with the risk appetite and risk tolerance. The role becomes more operational when the internal audit function drafts policies or recommends particular risk responses, though management's responsibility for risk decisions should be clearly understood by all parties.
- **Monitor:**
  The internal audit function maintains a dynamic view of significant risks to the organization to prioritize its assurance and advisory services. It also monitors management's progress on actions to address risks identified in assurance engagements. The role becomes more extended when the internal audit function is asked to develop and/or monitor risk indicators for management, track mitigation efforts arising from ERM activities, or perform ongoing second-line support activities.
- **Report:**
  The internal audit function provides assurance reporting to the board on the effectiveness of risk management, compliance, and control processes. The role becomes broader where the internal audit function consolidates or prepares enterprise risk reports on behalf of senior management.

This scenario does not imply that expanded roles for internal auditors are inherently ineffective or undesirable. In certain contexts, they may be practical or transitional. As governance and management structures evolve, clarity about the impacts on the internal audit function's independence and objectivity due to operational involvement is essential to implement appropriate safeguards and maintain confidence in future assurance.

In practice, this scenario requires explicit governance safeguards, which may include:

- The board should formally approve the expanded responsibilities, with clear articulation of scope and rationale.
- Responsibilities must be clearly documented in the internal audit charter, distinguishing between advisory facilitation and operational ownership.
- Internal auditors must not provide assurance over activities they have designed, operated, or managed until after 12 months have passed from the last action or responsibility.
- Independent and objective assurance, either from another internal function or an external provider, should be arranged for the affected areas.
- The arrangement should be periodically reviewed to determine whether ERM responsibilities can transition fully to management or a dedicated second-line function.

This scenario may be transitional or exceptional, rather than permanent. The objective should remain a clear separation of responsibility for risk response decisions and independent assurance of risk management and compliance activities.

Scenario B: The Chief Audit Executive Supervises a Risk Management Function

The chief audit executive may have supervisory responsibility for a separate risk management function, while the internal audit function remains organizationally and operationally distinct. In this structure, the chief audit executive is viewed as having sufficient knowledge and leadership skills to manage both functions while ensuring that they fulfill their separate purposes.

This arrangement can strengthen coordination, align risk and assurance perspectives, and improve enterprise-level visibility. However, even when operational roles are clearly separated, the shared reporting structure may raise perceived objectivity concerns. The key governance question is whether the internal audit function's independence and objectivity are effectively preserved in practice.

Viewed across the ERM cycle, this scenario may appear as:

- **Identify:**
  The risk management function leads organizationwide risk identification and maintains the risk taxonomy. The internal audit function may independently perform risk identification for audit planning purposes, or it may rely to some extent on the risk management function's efforts. While operational execution and use of the framework may remain separate, the shared supervision may raise questions about whether the internal audit function's view of risk is fully independent from the risk management function.
- **Assess:**
  The risk management function designs and applies risk assessment methodologies and scoring models. The internal audit function does not operate these processes, but may consider their outputs when determining audit priorities. The sensitivity here lies in whether stakeholders perceive audit planning decisions as sufficiently independent and objective, despite the fact that second-line efforts are supervised by the chief audit executive.
- **Manage:**
  Management, supported by ERM, determines risk responses within the risk appetite and risk tolerance. Internal auditors do not participate in these decisions. However, when the chief audit executive supervises a risk management function, there may be concerns that the internal audit function's later evaluation of risk management activities could be influenced — directly or indirectly — by leadership alignment.

- **Monitor:**
  The risk management function monitors key risk indicators and mitigation activities. The internal audit function evaluates whether monitoring processes are effective. Although execution is separate, stakeholders may question whether internal auditors can fully challenge the effectiveness of processes supervised within the same reporting structure.
- **Report:**
  The risk management function prepares enterprise risk reports for senior management and the board. The internal audit function provides its own assurance reporting. Even without direct involvement in drafting risk reports, the shared reporting line may create the perception of reduced distance between risk reporting and assurance.

In this scenario, the technical, formal separation between execution and assurance may be intact. However, the possible perception of impairment requires recognizing and understanding these sensitivities to maintain stakeholder confidence in the objectivity of internal auditors and the chief audit executive.

Preserving the internal audit function's independence and objectivity in this scenario depends on structural clarity. This scenario can function effectively when transparency and structural safeguards are in place. Supervision of ERM activities does not equate to ownership of risk management or compliance decisions, and assurance activities can remain independent in performance and reporting.

Good Practices: Integrated Assurance

In some organizations, coordination and reliance evolve into a more structured and deliberate model commonly referred to as integrated assurance. The concept of integrated assurance may be understood as a formalized approach that aligns, maps, and communicates assurance and advisory activities across the organization in a coordinated manner to provide a coherent view of governance, risk management, compliance, and control effectiveness.

Integrated assurance represents a mature form of coordination and reliance that organizations may find beneficial as risk environments grow more complex and interconnected. Its design and implementation should reflect organizational context, risk profile, and governance expectations.

Rather than operating in parallel silos, assurance providers — including management monitoring activities, second-line roles, the internal audit function, and in some cases external assurance — may align methodologies, share risk information, and coordinate planning cycles. This can result in greater transparency over coverage, reduced duplication of effort, and a clearer articulation of where assurance is sufficient and where gaps may exist.

In practice, integrated assurance may involve developing a structured assurance map, shared risk taxonomies, aligned reporting formats, or coordinated planning discussions among assurance providers. The chief audit executive and internal auditors are best placed to facilitate or coordinate roles in such arrangements, given their organizationwide perspective and direct reporting line to the board. However, such efforts can remain focused on promoting clarity and coherence without assuming ownership of second-line activities. Even with coherence, the chief audit executive must continue to challenge or highlight where information from the first and second lines is inaccurate, incomplete, or unreliable.

Integrated assurance can strengthen governance, risk management, and compliance by providing the board and senior management with a more comprehensive and synthesized view of assurance across significant risks. It may enhance efficiency, improve consistency in risk language and reporting, and support more informed oversight and strategic discussions. Even with integrated assurance, senior management remains accountable to the board for risk management and compliance, and the independence and objectivity of the internal audit function must be preserved.

Glossary

Definitions are mainly adapted from the glossary in The IIA's Global Internal Audit Standards.

advice – Information provided to an organization's stakeholders without providing assurance or taking on management responsibilities.

assurance – Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, compliance, and control processes.

assurance map – A high-level document that identifies the holistic risk coverage across the organization by a range of assurance providers. It helps to identify gaps in and duplication of assurance coverage.

board – Highest-level body charged with governance, such as:

- A board of directors.
- A board of governors or trustees.
- A group of elected officials or political appointees.
- Another body that has authority over the relevant governance functions.

In an organization that has more than one governing body, "board" refers to the body/bodies authorized to provide management and the internal audit function with the appropriate authority, roles, and responsibilities.

If none of the above exist, "board" should be read as referring to the group or person that acts as the organization's highest-level board. The board may delegate certain responsibilities to a committee, such as an audit committee.

chief audit executive – Term used to refer to the head of the internal audit function in an organization. The specific job title and/or responsibilities may vary across organizations.

compliance – Adherence to laws, regulations, contracts, policies, procedures, and other requirements.

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.

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.

risk appetite – The types and amount of risk that an organization is willing to accept in the pursuit of its strategies and objectives. The board establishes the organization's risk appetite.

risk management – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

risk tolerance – Acceptable variations in performance related to achieving objectives.

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.

About The Institute of Internal Auditors

The IIA is an international professional association that serves more than 265,000 global members and has awarded more than 220,000 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***.

About Statements of Position

Statements of Position communicate The IIA's official stance and vision on critical topics affecting governance, risk management, compliance, and control. They explain how a subject should be interpreted or applied in the context of internal auditing and are used to influence regulators, standard setters, boards, and executives.

This document is principles-based and does not prescribe organizational structures. It should be applied using professional judgment, considering the organization's context, complexity, and governance needs. The Statements of Position are not part of The IIA's International Professional Practices Framework® because they are intended for an executive audience, rather than primarily for internal auditors.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

The Institute of
Internal Auditors

1035 Greenwood Blvd., Ste. 401
Lake Mary, FL 32746 USA
theiia.org