FUAD KALASHLI

Assumable Risk Management Responsibilities of Internal Audit in the Second Line of Defense

AGENDA

1. Introduction: Three Lines of Defense for Risk Management
2. Effective Risk Management and Internal Audit’s Evolving Role
3. The Key Risk Management Responsibilities Internal Audit Can Assume in the Second Line
3. Benefits of Internal Audit’s Involvement in the Second Line
5. Balancing Independence with Involvement
6. Conclusion and Key Takeaways

Q&A

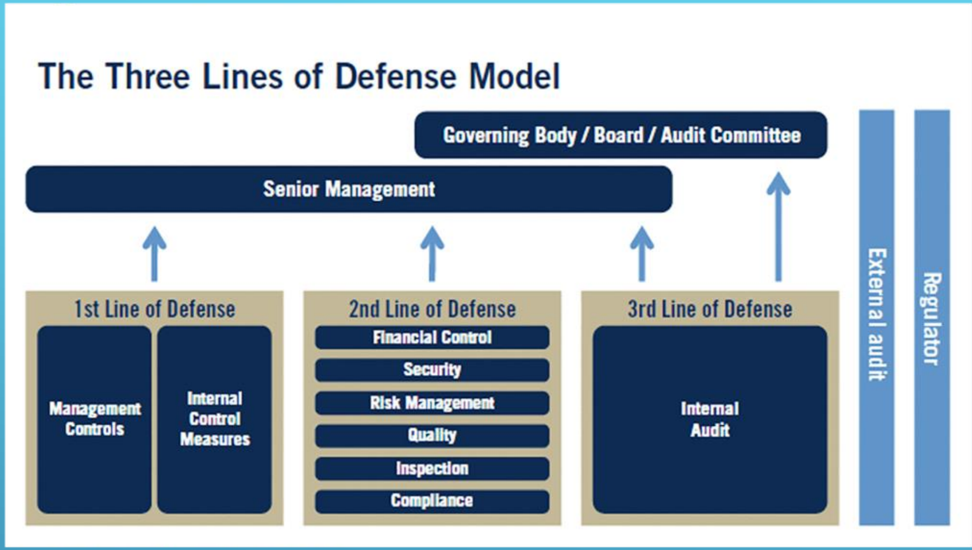
THE THREE LINES MODEL

The Institute of Internal Auditors (IIA) introduced the Three Lines of Defense model in 2013, adapted from the ECIIA/FERMA guidance based on Article 41 of the 8th EU Company Law Directive.

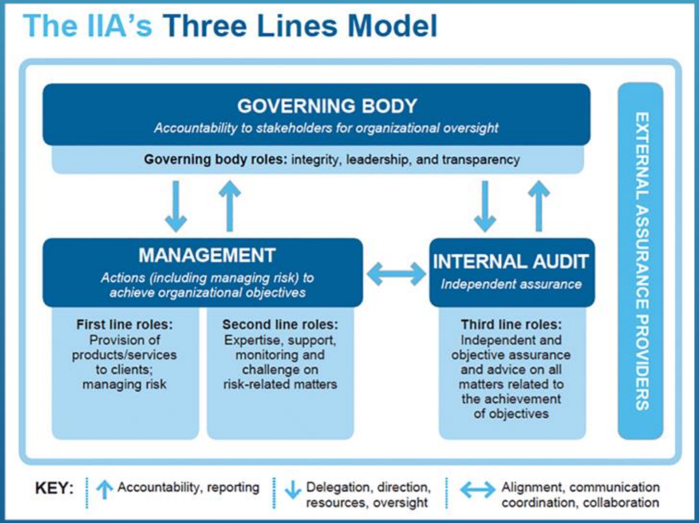
This model has since become a fundamental framework for risk management and control across organizations, particularly for governing bodies and the internal audit profession. It provides a structured approach to defining roles and responsibilities in managing risk and ensuring internal control, and has been widely adopted as a benchmark, especially in sectors with high regulatory oversight.

The **Three Lines of Defense (3LoD)** model is more than just a structural framework – it is a **strategic risk governance philosophy** that promotes clarity, accountability, and coordination across an organization's risk ecosystem

Original Model: 2013



Updated Model: 2020



The IIA's Three Lines Model: An update of the Three Lines of Defense

Initially, the model was designed to be generally applicable across all types of organizations, but it did not fully account for the unique requirements of specific industries such as regulated financial institutions. Recognizing the need for a more adaptive and collaborative approach, the IIA updated the model in 2020, renaming it the "Three Lines Model." This revision introduced a more flexible, principles-based structure aimed at fostering stronger alignment and cooperation between business functions and internal audit.

The paper was updated in September 2024 to reflect the new Global Internal Audit Standards glossary.

Not All Organizations Fit the Model Neatly

- In small or mid-sized organizations, **resource constraints** blur the boundaries between lines.
- **Dual-hatting** is common – where personnel wear both first and second line hats, or risk and audit responsibilities overlap.

Some critics of the old model said that the concept of risk had become dated; use of the term lines suggested silos and hard lines that could not be crossed; the lines alluded to sequential operations – first to second to third; the positioning of the board in the old graphic made it look remote, floating above the organization; it boxed in internal audit, as if saying 'you can't do that, you are third line'; it did not seem flexible for smaller organizations, the public sector, and non-regulated organizations; it left internal auditors wondering about so-called "blurring" of the lines and what it means when the chief audit executive (CAE) takes on roles outside of internal audit.

"GLOBAL PERSPECTIVES AND INSIGHTS The Three Lines Model – An Important Tool for the Success of Every Organization"

The 2020 IIA Update – More Than a Renaming

The IIA's revised **Three Lines Model (2020)** isn't just a rebrand – it:

- Centers **governance and accountability** as the unifying force
- Encourages **collaborative intelligence** across lines
- Promotes **strategic alignment of risk, compliance, and assurance**

Why the Model Matters

The model fosters clear communication, accountability, and coordination among different organizational levels. It helps avoid overlaps and gaps in risk oversight, promoting a comprehensive and consistent approach.

The Three Lines Model encourages a principles-based approach to match the needs and circumstances of an organization. Clearly, all organizations are different and there can be no one-size-fits-all approach. This led to the model's explicitly defined six principles on which it is based. An additional significant change was in the use of language, eliminating the use of "lines" and instilling the idea of "roles." Defining the key roles and describing the relationships among those core roles in the new Three Lines Model confirms coordination and alignment are essential to ensure organizational coherence and avoid silos. Most importantly, the new model amplifies the critical need for assurance on the adequacy and effectiveness of risk responses, including controls, as a fundamental component of governance. This is achieved through the competent application of systematic and disciplined processes, expertise, and insight by internal audit

EFFECTIVE RISK MANAGEMENT AND INTERNAL AUDIT'S EVOLVING ROLE

Effective risk management requires a coordinated, organization-wide effort, one that involves clear roles, open communication, and strong collaboration across all functions responsible for managing risk. The **Three Lines Model** provides a simple and effective way to enhance communication on risk management and control by clarifying essential roles and duties. Effective risk management demands **collaboration across all three lines of defense-**operational management (first line), risk and compliance functions (second line), and internal audit (third line). As regulatory environments toughen and risks grow more complex (e.g., cybersecurity, ESG, emerging technologies), organizations often face resource and expertise constraints within their risk and compliance teams. Therefore, **close cooperation and information-sharing between the three lines** become critical to leveraging diverse expertise, avoiding duplication of efforts, and fostering a unified risk culture. This collaborative approach strengthens the organization's capacity to identify, assess, and respond to risks in an integrated, efficient, and effective manner.

Internal audit in its modern-day form evolved from the 1940s through a process of evolution:

› Checking – up to 1960s – Simple checking of transactions to ensure correctness that often involved checking 100% of transactions.

› Compliance – 1960s–1980s – Simple compliance audits of individual business activities and transactions with a cyclical approach to cover every organisation activity over a number of years.

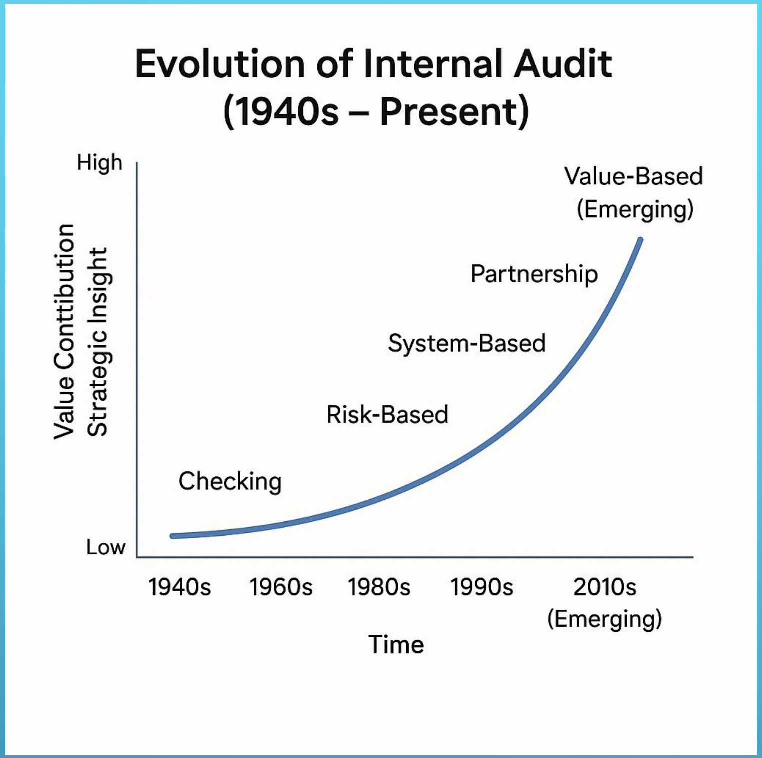
› System-Based – 1980s–1990s – Introduced the concept of end-to-end audits of system controls but maintained a cyclical approach to cover every organisation activity over a number of years.

› Risk-Based – 1990s–2010s – Internal audit accepted that limited budgets meant it could not audit everything, and also that some lower risk activities might not warrant the cost of an audit.

› Partnership – 2010s – Internal audit and management actively work together for the common good and success of their organisation, with internal audit maintaining its independence.

› Value-Based – emerging – A methodology where internal auditors perform forward-looking internal audit services to offer insights and actively seek innovation to improve an organisation, seeking to do this from the audit client perspective. Value-based auditing is where the internal audit profession is heading – not many internal audit functions are there yet, but it is an emerging trend.

"IIA-Australia White Paper - Internal Audit and Risk Management: Separate or Together?"



In this dynamic environment, **internal audit's role has evolved significantly**

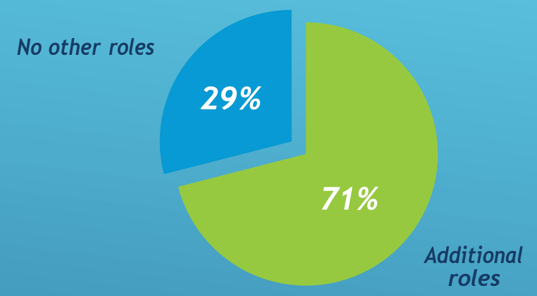
Then (Traditional View)	Now (Evolved View)
Retrospective	Forward-looking
Static audit plan	Agile, risk-responsive planning
Checks controls	Evaluates risk frameworks and culture
Works independently	Collaborates while staying independent
One-way communication	Two-way, cross-functional engagement
Primarily compliance	Strategic insight + assurance

Why Internal Audit's Role Is Evolving

- **Risk environment is more complex & interconnected**
  → Requires broader, system-wide audit perspective
- **Stakeholders demand strategic insight, not just assurance**
  → Boards expect forward-looking, value-adding risk advice
- **Governance frameworks promote collaboration**
  → Internal audit works more closely with the second line
- **Digital transformation & rapid change**
  → Internal Audit must adapt with agile methods, data analytics, and early engagement
- **Greater focus on risk culture & behavior**
  → Assessing ethics, tone at the top, and organizational mindset

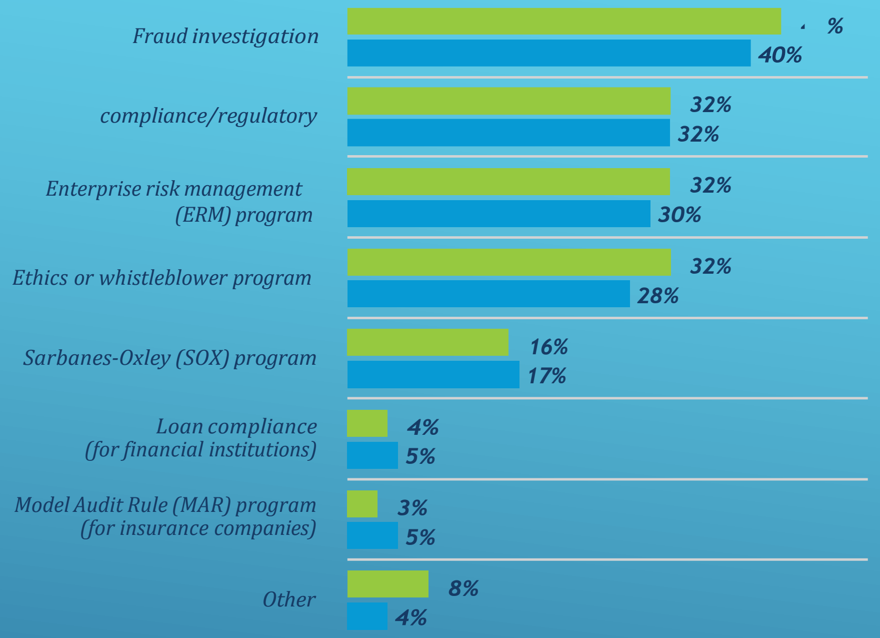
Seventy-one percent (71%) of CAEs and other senior-level internal auditors reported having responsibilities beyond their role as head of internal audit (refer to Figure 16).

Figure 16
Other Roles and Responsibilities



Source: Vision 2035 Survey. [cAEs; Other Senior-Level Internal Auditors] In addition to your role as head of internal audit, for which areas are you responsible?

Roles Beyond Internal Audit



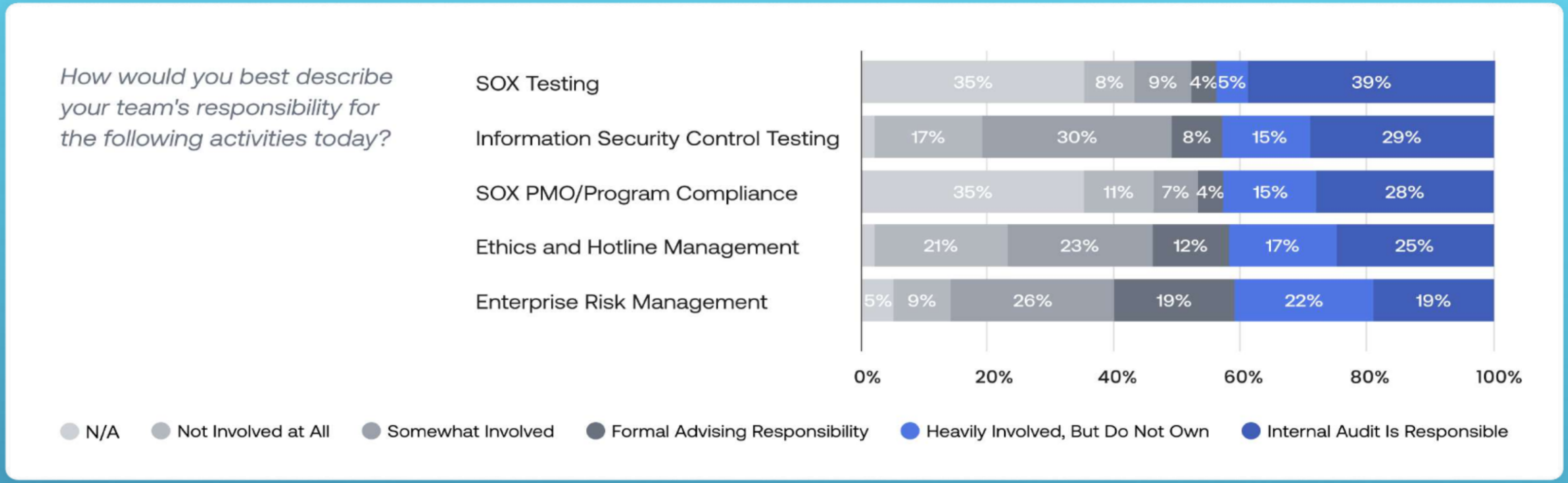
Despite their expanded responsibilities, senior leaders maintain internal audit's independence by adhering to the Standards, which call for implementing safeguards. The responsibilities of CAEs extending beyond internal audit have been documented in findings from other IIA surveys over the years. For instance, based on findings from The IIA's *North American Pulse of Internal Audit*, particularly from 2022 to 2024, CAEs reported having to manage areas such as fraud investigation, enterprise risk management, and others. Among the 71% of respondents from the Vision 2035 survey who reported having roles outside of internal audit, the top three areas for which they are responsible include fraud investigation (43%), compliance/regulatory matters (32%), and enterprise risk management (32%)

Even though internal audit remains the sole internal provider of independent and objective assurance on the adequacy and effectiveness of governance and risk management, some organizations continue to see synergies by including second-line function work within the scope of internal audit due to skill needs and cost considerations. In some cases, CAEs manage internal audit and other second-line functions like risk or compliance.

According to the IIA's North American Pulse of Internal Audit Survey (Oct–Nov 2024),

89% of Chief Audit Executives (CAEs) are responsible for one or more areas outside the traditional internal audit function. Reflecting this, the **2025 Pulse of Internal Audit report** shows that **over 55% of internal audit functions have already taken on or plan to take on more proactive risk management roles**, positioning internal audit as a strategic partner alongside risk and compliance functions. This shift highlights internal audit's expanding role—not only in assurance but also in advisory services, risk insight, and early involvement in the risk management process—thereby strengthening overall organizational risk resilience.

Top Five Responsibilities Beyond Traditional Internal Audit Work



AuditBoard's report, titled "Internal Audit's Expanding Role: The Foundation for Connected Risk,"

ERM ranked #5, with 41% of CAEs owning or heavily involved and another 19% formally advising. Now, consider that ERM is aligned with advisory in these responses — meaning that the 60% of CAEs who are owning, heavily involved, or formally advising in ERM

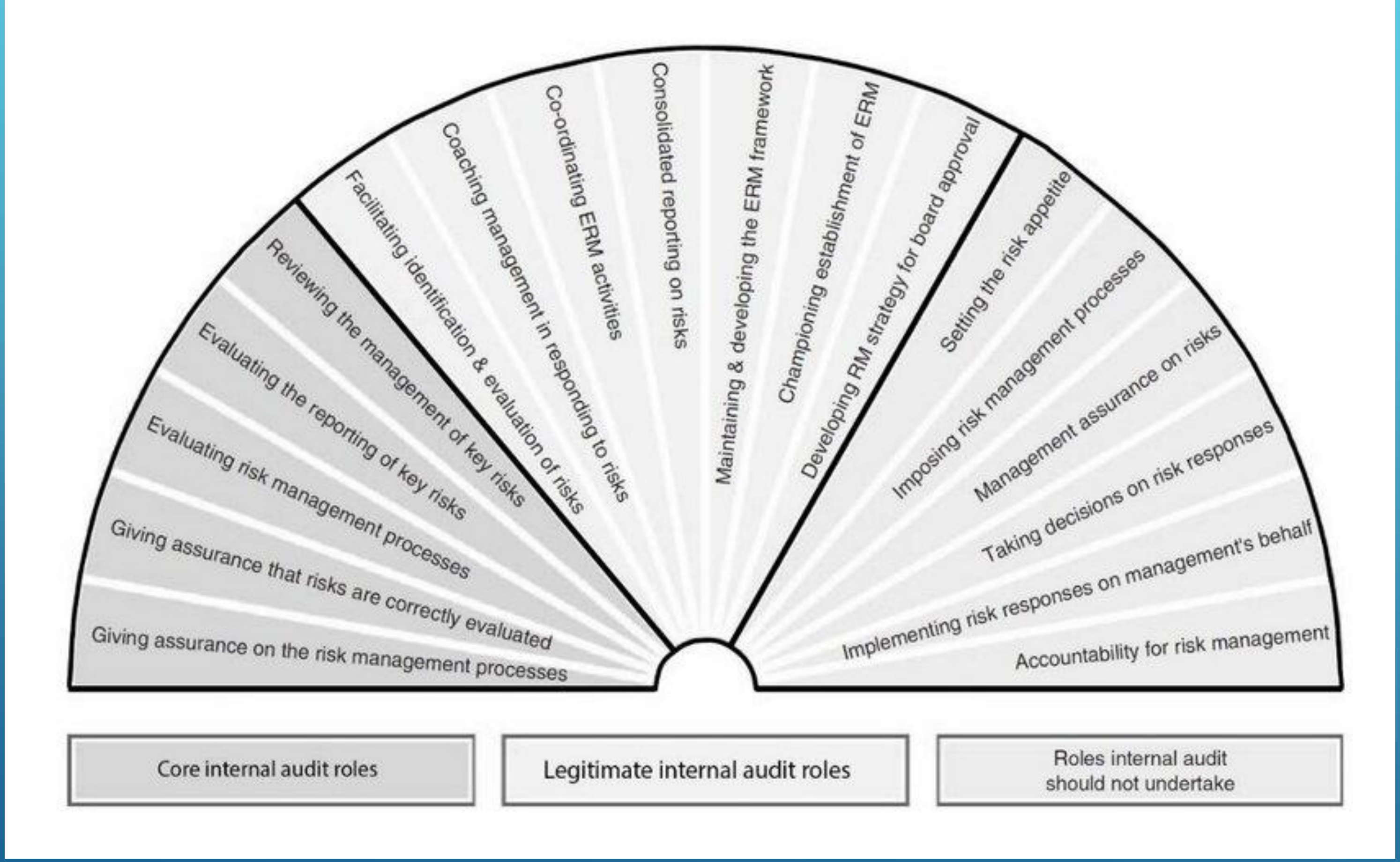
Top Five Areas Where CAEs Seek Greater Responsibilities

AuditBoard's report, titled "Internal Audit's Expanding Role: The Foundation for Connected Risk,"

IRM was CAEs' #1 choice for where they should be more involved. Notably, however, IRM is not even reflected in auditors' top existing responsibilities (see Figure 4), though it was an answer option. CAEs' #2 choice — ERM — is also telling. There seems to be a growing consensus that internal audit needs to level up its ERM game (e.g., limited involvement graduating to heavy involvement or even owning). In aggregate, these findings suggest:

- A need for greater overall risk focus from internal audit, since three of the top five areas relate to becoming more involved with risk work — IRM, ERM, and ORM

THE KEY RISK MANAGEMENT RESPONSIBILITIES INTERNAL AUDIT CAN ASSUME IN THE SECOND LINE



Internal auditing's role in ERM

According Position Paper **"The Role of Internal Auditing in Enterprise-Wide Risk Management":**

- Core Roles of Internal Audit in ERM (Appropriate Role)
- Legitimate Roles with Safeguards (May be Appropriate if No Impairment to Independence)
- Roles Internal Audit Should Not Undertake

Standards Spotlight

Standard 6.1 Internal Audit Mandate

Considerations for Implementation

Role(s) – The primary role of the internal audit function is to conduct internal audit activities and deliver internal audit services. There may be situations where roles beyond internal auditing are part of the chief audit executive’s responsibilities, such as risk management or compliance. These nonaudit roles are discussed further in Standard 7.1 Organizational Independence

Standard 7.1 Organizational Independence

Requirements

When the chief audit executive has one or more ongoing roles beyond internal auditing, the responsibilities, nature of work, and established safeguards must be documented in the internal audit charter. If those areas of responsibility are subject to internal auditing, alternative processes to obtain assurance must be established, such as contracting with an objective, competent external assurance provider that reports independently to the board.

When the chief audit executive’s nonaudit responsibilities are temporary, assurance for those areas must be provided by an independent third party during the temporary assignment and for the subsequent 12 months. Also, the chief audit executive must establish a plan to transition those responsibilities to management.

Standards Spotlight

Standard 7.1 Organizational Independence

Considerations for Implementation

In addition to the responsibilities of managing the internal audit function, the chief audit executive is sometimes asked to take on nonaudit roles that may impair or appear to impair the internal audit function's independence. Examples include situations such as:

- A new regulatory requirement prompts an immediate need to develop controls and other risk management activities to ensure compliance.
- The chief audit executive has the most appropriate expertise to adapt existing risk management activities to a new business segment or geographic market.
- The organization's resources are too constrained or the organization is too small to afford a separate compliance function.

The CAE may be asked to assume second line of defense activities in situations such as:

 New regulatory requirement: A new regulation requires substantial effort associated with new policies, procedures, testing, and risk management activities.

 Change in business: An organization may enter into a new geographical market or new business segment and be subject to new regulations or risk management activities.

 Resource constraints: An organization may experience resource constraints or changes in staff, such as when the leader of a second line of defense function leaves the organization.

 Efficiency: Management and/or the board may determine it is more efficient for internal audit to perform compliance or other second line of defense functions.

Internal Audit's Core Assurance Roles

- Provide assurance on the risk management process.
- Provide assurance that risks are correctly evaluated.
- Evaluate the reporting of key risks.

- Review the management of key risks (including testing controls).

Internal audit's roles with safeguards

- Facilitate identification and evaluation of risks.
- Coach management in responding to risks.
- Coordinate ERM activities.
- Consolidate reporting on risk.
- Champion establishment of ERM.

Roles internal audit should not undertake

- Setting risk appetite.
- Imposing risk management processes.
- Providing management assurances on risk.
- Making decisions on risk responses.
- Implementing risk responses on management's behalf.
- Assuming accountability for risk management.

BENEFITS OF INTERNAL AUDIT'S INVOLVEMENT IN THE SECOND LINE

Internal Audit's active participation in the second line of defense goes beyond traditional assurance roles and brings substantial value to an organization's risk management framework. By collaborating closely with risk management and control functions, Internal Audit helps enhance the effectiveness and efficiency of risk oversight. This involvement leads to improved early risk detection, stronger governance, and a more proactive risk culture. In addition, Internal Audit's unique perspective and skillset help reduce duplicative efforts and enable joint risk assessments, fostering a more integrated and dynamic risk management environment. The following points highlight the key benefits organizations can realize when Internal Audit assumes responsibilities in the second line.

Internal Audit's involvement also leads to the harmonization of risk assessment methodologies and the elimination of redundant assurance activities, promoting efficiency and clarity. It empowers organizations to adopt dynamic risk management practices, allowing real-time recalibration of controls in response to changing business environments.

Benefits to the Internal Audit Function

- **Broader Impact:** Internal audit's role extends beyond traditional focuses on compliance and financial statement accuracy, allowing the function to influence a wider range of organizational risks and processes.
- **More Robust and Relevant Audit Plan:** Involvement in the second line helps internal audit develop audit plans that better reflect current and emerging risks, increasing the relevance and value of audit activities.
- **Increased Knowledge and Expertise:** Active participation in second-line functions provides internal audit staff with growth and training opportunities, enhancing their risk management skills and overall professional development.

Benefits to the Organization

Holistic Risk Insights Through Integrated Risk Assessment

Internal audit brings cross-process insights that enrich second-line risk assessments. For instance, internal audit's deep dive into financial controls can reveal operational or compliance risks that risk managers might not prioritize. By integrating audit findings into risk registers, the second line gains a more comprehensive understanding of risk exposures.

Enhanced Risk Identification and Early Warning Capabilities

Internal audit teams often have a broad view of organizational processes and risks through their periodic audits. When involved in the second line, they can contribute to real-time risk identification rather than just retrospective reviews. Their expertise in control weaknesses helps the risk management function to focus on critical and emerging risks proactively, providing a more dynamic risk profile.

For example, internal audit involvement in risk workshops or risk assessments brings a fresh perspective that operational risk managers might overlook, especially in complex or cross-functional areas.

Increased Efficiency and Reduced Duplication

Often, risk management, compliance, and internal audit functions may conduct overlapping activities such as risk assessments and control testing. By aligning internal audit activities within the second line, organizations can reduce redundant work, optimize resource allocation, and lower operational costs. This synergy leads to better data sharing and process integration.

Promoting a Proactive Risk Culture

Internal audit's active role in the second line helps cultivate a proactive risk culture across the organization. By engaging early with business units on risk awareness, controls, and compliance, internal audit encourages employees to identify and address risks before they escalate. This cultural shift reduces risk tolerance for non-compliance or control failures and embeds risk management as a core aspect of everyday decision-making.

BALANCING INDEPENDENCE WITH INVOLVEMENT

Standards Spotlight

Standard 7.1 Organizational Independence

Considerations for Implementation

When discussing nonaudit roles and responsibilities with the board and senior management, the chief audit executive should identify appropriate safeguards depending on whether the roles are permanent or temporary and intended to be transferred to management.

When the board agrees that an impairment has occurred, the chief audit executive should suggest to the board and senior management potential safeguards to manage the risks. It is also important to specify a timeline for transitioning temporary nonaudit responsibilities to management.

The requirement is to have assurance activities overseen by an independent third party for the subsequent 12 months after the chief audit executive completes temporary responsibilities in that area. However, judgment should be used as there may be circumstances whereby the perception of impairment may exist beyond 12 months. The chief audit executive should discuss with the board and senior management whether 12 months is appropriate or not

Transition Plan

If the assignment of second line of defense responsibilities to internal audit is considered temporary, it may be beneficial to develop a formal transition plan, discuss it with management and the board, and implement it to eventually reassign those responsibilities. The transition plan can take into account factors such as:

- Organizational/structural needs: Internal audit may need to adjust reporting relationships as individuals or groups cease their role in second line of defense activities. If these responsibilities are moving elsewhere in the organization, structural changes may be required to ensure independence and objectivity.
- Resources: Resources may be required to train individuals elsewhere in the organization for second line of defense duties or to transition internal audit staff to these roles.
- Timeline and tasks: Responsibilities and target dates for key milestones should be documented.
- Maintaining independence during transition: In accordance with Standards, individuals must refrain from assessing specific matters for which they were previously responsible for a period of at least one year. This would apply to individuals who have been involved in second line of defense activities while working within internal audit.
- Monitoring progress: The CAE should monitor progress of the transition plan.
- Transparency: Ongoing communication with management and the board regarding adherence to the transition plan and schedule. Significant changes or delays should be evaluated and approved by the board.

Internal audit should take care to avoid activities that compromise their independence and/or objectivity, including:

- Setting the risk appetite.
- Owning or managing risks.
- Assuming responsibilities for accounting, business development, and other first line of defense functions.
- Making risk response decisions on management’s behalf.
- Implementing or assuming accountability for risk management or governance processes.
- Providing assurance on second line of defense activities performed by internal audit.

Formalization by documenting roles and responsibilities in the internal audit charter

It is important to avoid any ambiguity regarding the potential roles of Internal Audit and second line of defense functions in the organization by explicitly defining these roles. The aim, mandate and nature of the internal audit's activities should be documented in the organization's internal audit charter and be approved by the Management Board and the Audit Committee. If the Internal Audit is also responsible for one or more second line of defense functions, this should be explicitly stated in the charter, along with the role and responsibilities of the internal audit in this respect and the impact on the internal audit mandate.

CONCLUSION AND KEY TAKEAWAYS

Internal audit, with its holistic view across the organization, is increasingly recognized as a valuable contributor beyond its traditional third-line role. **By assuming clearly defined, advisory-focused responsibilities within the second line, internal audit can significantly enhance the organization's risk management capabilities** while still maintaining its independence and objectivity.

In conclusion, the assumable responsibilities of internal audit in the second line represent not a threat to independence, but an opportunity to lead. **By embracing this role with clarity, caution, and competence, internal audit can evolve into a cornerstone of proactive governance, trusted assurance, and enterprise-wide value creation**

Conclusion: Role Clarity = Risk Clarity

To fully support the organization while maintaining credibility, Internal Audit must:

- **Remain advisory, not operational.**
- **Document its boundaries.**
- **Secure governance approval and oversight.**
- **Continuously monitor and disclose the nature of its involvement.**

Key Takeaways

- **The Three Lines Model remains foundational**, but must be applied with flexibility to reflect today's dynamic risk environment and organizational realities.
- **Internal audit can play a vital role in the second line** by offering risk advisory support, reviewing and enhancing risk frameworks, fostering a strong risk culture, and supporting enterprise-wide risk assessments.
- **It is crucial that internal audit does not assume risk ownership.** Its role must remain independent, focused on providing assurance, insight, and constructive challenge—not on managing or mitigating risks directly.
- **Strong governance, clearly defined roles, and active oversight by the audit committee** are essential to safeguard internal audit's independence and maximize its effectiveness in a second-line support capacity.
- **A forward-looking, risk-aware internal audit function is a strategic enabler.** It supports better decision-making, enhances agility, and builds organizational resilience in the face of uncertainty.
- **The ultimate objective is balance**—delivering proactive and insightful risk support while preserving the clarity of roles and responsibilities across all lines of defense.

THANK YOU!