KPMG

Defining roles and responsibilities across the first, second, and third lines with limited resources

Today, companies operate in challenging business environments shaped by internal and external factors, making effective risk management increasingly complex. A KPMG survey from September 2024 conducted with risk and internal control professionals, highlights several critical pain points that many organizations encounter when striving to implement robust risk management practices. These include:

- **Blurred first, second, and third lines** with a lack of clarity between the roles and responsibilities of the second and third lines.
- **Accountability gaps** where unclear ownership of risks hinders effective oversight and action.
- **Balancing independence and capacity** as organizations struggle to maintain independence across the three lines while operating with limited staffing and resources.
- **Prioritization challenges** where resource constraints make it difficult to determine which risks to address first, leading to inefficiencies in risk mitigation efforts.
- **C-Level engagement challenges** including difficulties in embedding risk roles and responsibilities and securing strong support from executive leadership.
- **Inconsistent communication** resulting in poor collaboration and information sharing across lines, which creates gaps in risk oversight.

This article explores practical solutions to address these challenges focusing on the critical importance of defining roles and responsibilities within the three lines model. It delves into governance, efficiency, and cultural challenges and offers actionable strategies to address them, helping organizations maximize their risk management capabilities.

The importance of roles and responsibilities in the three lines model

Organizations oftentimes face difficulties in allocating roles and responsibilities across the three lines. However, a clear understanding of these roles and responsibilities is crucial for ensuring effective governance, risk management and control within the organization. This framework divides risk management responsibilities into three distinct lines, each with a specific purpose and scope:

- **The first line:** The business functions hold the responsibility for managing risks as part of their everyday activities. This line forms the foundation of risk management, requiring employees to identify, measure, manage, and report on risks directly at the operational level. For instance, a manufacturing supervisor implementing safety protocols to minimize workplace accidents exemplifies first line risk ownership.
- **The second line:** This, amongst others, encompasses risk management and compliance functions that establish policies, provide oversight, and guide the first line. The second line is responsible for facilitating and providing the risk framework for organizations, facilitating risk identification and assessment, and reporting to management and the board. For instance, a risk officer establishing guidelines to manage project delivery risks, such as delays or cost overruns, highlights the role of the second line.
- **The third line:** Internal audit provides independent assurance that the organization's risk management and control processes are functioning as intended. It evaluates whether the first and second lines are addressing risks effectively and in alignment with organizational goals. An internal audit team conducting a review of cybersecurity measures to ensure compliance with industry standards is a prime example of third line assurance.

When these roles are poorly defined, organizations risk encountering overlapping responsibilities or significant gaps in risk coverage. For example, confusion between the second and third lines over the scope of oversight versus assurance can lead to inefficiencies and overlooked risks. Furthermore, if risk ownership within the first line is not clearly assigned or positioned at the right organizational level, critical risks may remain unmanaged or improperly addressed.

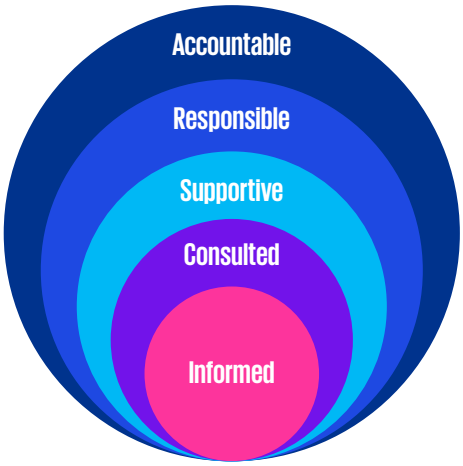
By establishing clear delineation of responsibilities, organizations can foster collaboration, avoid redundancies, and create a robust risk management framework aligned with their strategic objectives. In the following sections, we will further elaborate on how organizations can achieve this in practice.

Governance toolkit: Strengthening the framework

Effective governance is essential for the three lines model to function seamlessly. While defining roles and responsibilities is foundational, organizations also need structured methodologies to ensure alignment, minimize redundancies, and comprehensively address risks. Two key tools that can significantly enhance governance are the RACI matrix and assurance mapping, which provide clarity, structure, and focus in managing risk-related activities.

The RACI or RASCI matrix (Responsible, Accountable, Supportive, Consulted, Informed) are widely used frameworks for defining and documenting roles and responsibilities. By mapping tasks, processes, or decisions to specific individuals or teams, the matrix eliminates ambiguity and ensures accountability. Each activity is assigned four potential roles:

- **Accountable:** Has ultimate accountability over the service. Only one role/person can be accountable for a service. If no other party is shown as Responsible, the Accountable bears responsibility. Responsible for sign-off on deliverables unless this has been delegated to other individuals.
- **Responsible:** Has responsibility for the definition, production and delivery of the service including liaison with any party who is Accountable or Consulted. Can be responsible for facilitation of sign-off for deliverables and any other associated activities to enable this.
- **Supportive:** Provides resources, assistance, or expertise to aid in the delivery or execution of the service. This role does not hold responsibility for deliverables but plays a critical part in enabling the Responsible party to.
- **Consulted:** Has a responsibility to contribute with resources, information, comments, risks, challenges, or insight to help. Consulted parties are also considered to be Informed.
- **Informed:** Should actively be kept informed about the high-level performance and outcome of the service.



This structured approach fosters clarity and collaboration, preventing duplicated efforts and ensuring that each responsibility is explicitly owned. For example, in a project to implement new data privacy regulations, the RACI matrix might designate compliance officers as accountable for policy creation, operational managers as responsible for employee training, legal advisors as consulted, and senior executives as informed. This alignment streamlines processes and ensures all stakeholders understand their roles.

Another critical tool (which can be used as a complement to the RACI and RASCI) is assurance mapping, which aligns assurance activities—such as audits, risk assessments, and compliance checks—with an organization's key risk priorities. Assurance mapping provides a visual representation of oversight, identifying who monitors which risks and to what extent. This process not only highlights overlap in assurance efforts but also uncovers gaps where critical risks may be insufficiently addressed. The assurance mapping methodology involves three key steps:

- Identifying key risks and stakeholders to the organization;
- Assigning assurance providers from the three lines to each risk; and
- Creating a comprehensive map to visualize the scope and focus of assurance activities.

By doing so, organizations can allocate resources more effectively, ensuring that high-priority risks receive adequate attention without duplication of efforts. For instance, an assurance map might reveal overlapping efforts between the second line's risk management function and internal audit in assessing compliance with major regulatory changes, while uncovering gaps in monitoring emerging market risks or sustainability-related risks. This insight allows organizations to streamline efforts and prioritize assurance activities for the most critical strategic objectives.

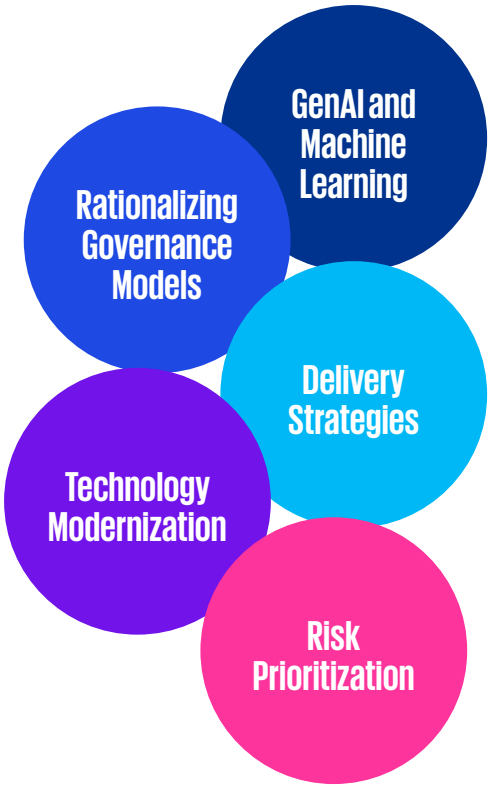
Principal Risks	Gross Risk Score	First Line of Defence Business operations "Management Controls"		Second Line of Defence Oversight functions, e.g. Risk, Compliance, Centrol Controls Office, Health and Safety etc				"Third Line of Defence Internal Audit"	"Fourth Line of Defence External Audit"
		Control Assurance/ QA	Independent Reviews	Risk	Compliance	Central Controls Office	Other		
Regulatory Risk	15	M	M	M	N/A	M	M	M	N/A
Operational Risk	8	H	H	L	N/A	H	H	N/A	N/A
People Risk	15	H	H	M	N/A	H	H	N/A	N/A
Financial Risk	9	H	M	L	N/A	M	M	N/A	M
Credit Risk	10	H	H	L	N/A	M	M	N/A	M
Liquidity Risk	8	M	M	M	N/A	N/A	M	N/A	M
Technology Risk	8	L	L	H	M	N/A	M	N/A	N/A
ESG Risk	12	H	M	M	M	H	M	N/A	N/A

By embedding these tools into the governance framework, organizations can enhance the effectiveness of the three lines model. This not only ensures better risk management but also fosters a proactive governance culture, where oversight becomes a strategic enabler rather than a compliance exercise.

Efficiency toolkit: Maximizing impact with limited resources

When resources are stretched thin, achieving efficiency without compromising risk management quality becomes paramount. By leveraging **innovative tools, modernizing technologies**, rationalizing **governance models**, and prioritizing efforts, organizations can enhance their risk oversight capabilities without overstretching their resources.

One innovative approach to achieving efficiency is the use of **generative AI** (GenAI) **and machine learning** (ML). These advanced tools streamline repetitive tasks, such as risk identification, internal control design, and process documentation. While generative AI can automate the creation of risk frameworks, control descriptions, and even initial assessments of new risk areas, machine learning focuses on continuous improvement through data-driven insights. For instance, ML algorithms can analyze historical risk data to identify emerging trends or predict future risk scenarios, helping teams to focus on higher-priority issues. Large Language Models (LLMs), another form of AI, excel at synthesizing vast amounts of textual information, allowing them to generate detailed reports, draft policies, or summarize key findings in risk assessments, which ultimately saves time and enhances accuracy. Together, these tools reduce manual workloads, ensure consistency in risk documentation, and enable scalability, allowing organizations to handle larger volumes of work without increasing headcount.



Another pillar of efficiency is **technology modernization**, which focuses on digitizing and automating risk management processes. Centralized data platforms act as a single source of truth, integrating risk data to eliminate duplication and ensure consistency across the organization. Automating workflows, such as risk reporting or control testing, reduces administrative burdens, enabling teams to dedicate more time to critical tasks like strategic risk management and mitigation planning.

When resources are constrained, **rationalizing governance models** and strategies becomes crucial for maintaining effective risk oversight without overburdening internal teams. This involves aligning risk and internal control (as well as compliance) accountabilities at different levels of the organization to eliminate redundancies and ensure clear ownership. By streamlining roles and responsibilities, organizations can improve efficiency and reduce the complexity of managing risks across different functions. Additionally, rationalizing product offerings and channel delivery strategies helps minimize variability in risk exposure and the efforts required to manage those risks. This focused approach ensures that internal teams can concentrate their resources on high-priority areas while maintaining a consistent and effective risk management framework.

Tailored governance **delivery strategies** can also provide flexibility, enabling organizations to adjust their risk management efforts based on capacity. These approaches help free up internal resources for high-priority tasks and provide access to external expertise when needed. For example, outsourcing expert risk assessments or control testing can relieve internal teams, allowing them to focus on critical risk management activities, while ensuring internal controls are thoroughly tested.

Finally, **prioritizing risks** based on their materiality and potential impact ensures that limited resources are directed to the most critical areas. By assessing the significance of each risk in relation to organizational objectives, organizations can concentrate their efforts on high-impact risks while maintaining baseline controls for less critical ones. This focused approach enhances oversight of principal risks and ensures that resources are not wasted on areas with minimal impact. For instance, prioritizing operational risks that could disrupt supply chains or critical processes enables organizations to address vulnerabilities that could significantly affect business continuity.

Culture toolkit: Building a risk-aware organization

A **risk-aware and strong risk culture** is the backbone of an effective three lines framework. Without it, even the most well-designed governance and efficiency strategies are unlikely to succeed. Building such a culture requires concerted efforts to align leadership and employees on the importance of integrating risk management into everyday activities.

Driving engagement at the leadership level is critical, as decision-makers significantly shape the organization's risk profile and play a central role in defining its risk appetite. When executives clearly articulate the organization's tolerance for risk and actively model risk-conscious behaviors, they set a tone that cascades through the organization. This can be achieved by linking risk management efforts to strategic objectives, demonstrating how effective risk oversight enables the organization to achieve its goals. For example, illustrating how identifying emerging market risks early allowed the organization to adapt its strategy and seize new opportunities can showcase how risk management supports business growth and resilience. This can solidify leadership buy-in and commitment to embedding risk considerations into decision-making processes.

Additionally, the second line plays a crucial role in demonstrating its **strategic value**. By providing insights based on key performance indicators (KPIs) and key risk indicators (KRIs), the second line can show how proactive risk management directly impacts organizational performance. For instance, tracking trends in operational disruptions can reveal areas requiring immediate attention and illustrate the second line's contribution to business continuity.

At the operational level, fostering a risk-aware culture involves embedding risk considerations into the core activities of the first line such as projects, product launches, and day-to-day operations. Employees should see risk management as an integral part of their responsibilities rather than a compliance task. This can be achieved through consistent communication and training that highlights the practical relevance of risk management to their roles. For example, risk workshops tailored to specific projects or e-learning modules on identifying and managing risks during product development can build awareness. Furthermore, recognizing and rewarding risk-aware behaviors—such as anticipating potential project delays due to supply chain risks—encourages proactive engagement. By integrating risk into the operational function of the organization, the first line becomes an active driver of resilience and success.

Conclusion

In conclusion, implementing the three lines framework requires a multifaceted approach that brings together several solutions that go hand in hand to optimize second-line functioning and maximize its impact across the organization. Governance is the foundation, ensuring clear role definitions, accountability, and alignment across the three lines. Efficiency initiatives, such as leveraging innovative technologies and streamlining processes, enable the second line to focus on high-value activities while reducing redundancies. Cultural alignment reinforces these efforts by fostering a shared understanding of risk responsibilities and embedding risk awareness into decision-making at every level.

For resource-constrained organizations, prioritizing these initiatives becomes even more critical. By focusing on governance, efficiency, and cultural alignment, organizations can not only build resilient frameworks, but also ensure that their risk management practices support strategic goals and enhance overall organizational performance. Together, these solutions create a risk management system capable of navigating today's complex risk landscap

How KPMG can help

At KPMG, we stand ready to support organizations in the setup of their risk management activities, providing guidance, insights, and tailored solutions to address their specific challenges and objectives. This includes maturity assessments and implementation support in strategic and operational risk management activities, such as developing of risk charters, policies, and procedures, facilitating risk workshops, implementing internal control frameworks, and designing reporting formats.

In addition, we offer specialized expertise through our KPMG Powered Target Operating Models, helping organizations streamline risk management processes, prioritize resources effectively, and create alignment at all levels. This ensures that your risk management activities drive meaningful impact while aligning with organizational goals.

Contact

Olivier Elst
Partner
Enterprise Risk Services

M: +32 485 17 83 48
E: oelst@kpmg.com

Raphaël Schair
Principal
Enterprise Risk and Assurance

M: +32 498 21 07 04
E: rschair@kpmg.com

Naomi Kerremans
Senior Manager
Enterprise Risk and Assurance

M: +32 472 54 14 99
E: nkerremans@kpmg.com

kpmg.com/be