Taking ERM to the next level

By elevating the ERM function, audit committees can help organizations better manage risk and improve resiliency

By Edouard Bertin-Mourot

As companies navigate the next normal and grapple with the lingering effects of the pandemic, Enterprise Risk Management (ERM) has risen to the top of the audit committee agenda. ERM is essential in helping organizations better understand and proactively integrate risk and opportunity considerations into everything they do. But to do this successfully, organizations need to rethink the mandate and attributes of the ERM function—and this is where audit committees have a critical role to play.

Catalysts for change

The pandemic did not impact all organizations and industries equally. Some industries had to transform their business models or perform a hard reset because of permanent or long-lasting market changes. Other industries have benefitted from new customer behaviours and have seen exponential growth. Risk and uncertainty are simply a part of doing business. COVID-19 accelerated emerging trends while creating new ones and will likely be remembered as one of the most significant catalysts of business change in modern times. Organizations are not necessarily facing new risks; rather, multiple risks are operating in tandem and many organizations are inadequately prepared.

For audit committees, some of the common systemic risks that should be on the 2022 agenda include:

People, mental health, and well-being: The single greatest threat organizations face in managing their workforce is attracting and retaining talent. Across industries, attrition levels are reported at an all-time high as employees quit en masse for reasons ranging from burnout and 'pandemic epiphanies' to a desire to continue working remotely. The acceleration of a 'digital workforce' has also created increased employee isolation and an 'always on' culture. Organizations will need to develop new strategies to support employees' mental health and nurture a strong corporate culture within virtual and hybrid environments.

> The ERM function cannot take on a simple 'middle or back office' role. It has to be repositioned and empowered to make a difference and help the organization become collectively 'more risk confident'

Edouard Bertin-Mourot
Partner, Risk Consulting
KPMG in Canada

Environmental, Social and Governance (ESG): Sustainability is rapidly becoming more than just a reporting requirement. Understanding and integrating ESG into an organization's internal processes, protocols and governance is key to mitigating reputational and operational risks. ESG must be embedded in the organization's DNA.

Supply chain: Global supply chain disruptions are affecting the economy with ripple effects across industries. Relying on a single supplier can leave your organization vulnerable. Next generation supply chains will need to evolve and organizations will need to make their networks more resilient to future disruptions.

Disruption: Disruptive technologies—such as artificial intelligence, cryptocurrency, metaverse and other digital innovations—are the new norm and organizations that don't adapt or evolve could fail.

Cyber and Data Privacy: Data privacy and cybersecurity concerns are at an all-time high. Although some employees are gradually returning to the office, many will likely continue to work from home or in a hybrid work arrangement. Audit committees should ensure that management has plugged any gaps in data security, especially for hybrid/remote work procedures.

The rise of the ERM function

In this environment, organizations can't afford to solely react and improvise. Risk management is an essential component of any organization's ecosystem. An organization's ERM program should consist of interrelated components that work together to ensure proper management practices and oversight, including:

Governance: An effective ERM function can help an organization to better manage risk – from helping to ensure risk policies and procedures are adequate and in place across all major risk classes to harmonizing threat and risk assessment methodologies and practices. Risk appetite statements and metrics should be reviewed often, to shift away from an 'academic exercise' to truly informing strategy-setting and performance.

Independent review and challenge: The ERM function provides further confidence that risks are being adequately managed across the organization. It should be proactively integrated into business activities, rather than engaged downstream or after decisions are made. This can be achieved by partnering with the business or providing objective challenges on risk assessments performed by the business. Some common integration opportunities include strategic planning, change management and vendor risk management; while others are more industry-specific like model validation, investment risk management or new product approvals.

What should audit committees be asking?

- What is the ERM mandate and how does it support our strategic objectives?
- How is the ERM function empowered by the audit committee to drive the risk agenda?
- How coordinated is our organization in managing various risk classes?
- How does risk management help inform decision-making?

Advisory: The ERM function plays a true 'risk advisory' role by sharing expertise on the risk-return optimization discussions, providing a risk-based framework to support decision-making, evaluating the resilience of the organization to extreme stress events, and providing stakeholders with additional risk insights such as transversal risk analysis and risk and control good practices. When fully leveraged, ERM can deliver substantial value as organizations deliver on their objectives.

Setting up ERM for success

Risks don't operate in isolation. Rather, they are part of a highly interconnected network. That means they should be managed collectively with greater convergence between various risk-related programs such as ERM, ESG or vendor risk management. Integration and convergence help to reduce silos and potential misalignments between existing programs. This can be done by regrouping some of these functions—such as ERM and ESG under a Chief Risk Officer—or better bridging these separate functions.

As organizations grow and mature, the challenge is to find an equilibrium between the three Lines of Defense (LOD). The frontlines may perceive these activities as constrictive or burdensome—a sentiment that may be further magnified if requests and processes between the second and third LOD are viewed as redundant or duplicative. As such, organizations should look at new ways for the second and third LOD to collectively plan, rationalize and streamline efforts based on materiality and minimize overlap.

To be successful, the ERM function should have a clear and approved mandate and be empowered to drive the risk agenda; it's not another 'middle/back office' activity but rather a function that is increasingly expected to add value and provide insights for its stakeholders, including the audit committee.

Contact

Edouard Bertin-Mourot
Partner, Risk Consulting
KPMG in Canada
416-777-3511
edouardbertinmourot@kpmg.ca

Let's do this. home.kpmg/ca/audit