Building enterprise resilience and productivity amid unprecedented disruption

Audit committees play a key role in maintaining organizational resilience through risk governance and innovation oversight.

Organizations are navigating unprecedented disruption, driven by rapid market shifts, economic uncertainty, and transformative technologies. In this volatile environment where risks are interconnected and unpredictable, building enterprise resilience is essential for sustaining performance and growth. Resilience increasingly depends on shifting from reactive responses to scenario planning and predictive risk management that anticipates future risks, tests organizational readiness, and informs timely decisions. Audit committees are central to ensuring organizations remain resilient by guiding proactive risk governance while advancing productivity through oversight of transformation, AI adoption, and workforce upskilling.

> Audit committees must look beyond immediately identifiable risks and gain a firm understanding of the second- and third-order risks of events that could potentially impact the enterprise capability to serve its client base.

Akber Merchant
Partner, Regulatory and Risk Advisory (RRA), KPMG in Canada

Geopolitical risk as a major disruptor

Geopolitics has emerged as a dominant force driving global economic volatility. In 2024, the world saw the highest number of armed conflicts since 1946, disrupting supply chains, trade flows, and global markets.[1] Throughout 2025, U.S. tariff announcements fueled significant market turbulence, with volatility reminiscent of the early COVID-19 pandemic.

As the U.S. resets trade relationships, Canadian organizations across the spectrum have felt the impact directly, with U.S. tariffs disrupting revenues and supply chains and damping the national economic outlook. According to our 2025 CEO Outlook survey, supply chain resilience is the top concern for Canadian CEOs.[2] This volatility has influenced financing preferences, slowed business investment and hiring, and led banks to moderate loan growth.

[1] Uppsala Universitet. "UCDP: Sharp increase in conflicts and wars". Accessed November 4, 2025.
[2] KPMG in Canada. "Leadership in the breach". Accessed October 20, 2025.

Audit committees should ask management about the organizations structured scenario planning and predictive risk practices, shifting away from reactive responses, testing multiple geopolitical scenario exercises such as tariff regimes, supply chain chokepoints, capital controls, and pre-defining triggers, actions, and owners.

Audit committees must ensure management assesses the implications of current and future geopolitical events and conducts geographic risk-mapping to understand their effects on operations, supply chains, and markets with corresponding contingency planning. For instance, running regular, data-driven scenarios with clear cases and stress parameters, supported by integrated data and analytics, to ensure playbooks are informed by forward-looking signals rather than historical patterns. As such, organizations should maintain a well-defined geopolitical risk playbook linked to scenario triggers and response tiers that can be activated as signals emerge, enabling faster, pre-authorized decisions across the organization.

Technology, climate, and the intensifying risk landscape

Beyond geopolitics, organizations face escalating threats from technology and climate-related disruptions. Cyber-attacks continue to plague organizations as threat actors employ technologies such as AI, to create new and ever-sophisticated tactics. AI is disrupting nearly every organization, bringing new risks with its opportunities. Audit committees should understand where and how AI is being used across the organization, including tools under development and AI introduced via upgrades to technologies, to surface hidden dependencies and risks.

Climate risks are also increasingly materializing in financial statements, with extreme weather

Questions audit committees should be asking:

- Does the organization stress test its long-term strategy and capital allocation models against a range of potential geopolitical shocks such trade decoupling or regional conflicts?
- Is management properly identifying and managing the second- and third-order risks arising from events and innovations?
- Does the organization have real-time visibility into the concentration of risk among key technology vendors, especially those providing AI services, and what is the plan if a critical vendor fails?
- Does management understand how the integration of new technologies into the organization's systems and procedures will affect existing controls?
- Is quarterly reporting enough, or do we need interim deep dives on certain scenario testing?
- Do we have the right skill set on the audit committee to assess new areas of risk and the methodologies used to measure them?

affecting operations, supply chains, and insurance coverage. 93 per cent of Canadian business decision-makers surveyed expect their companies to be exposed to extreme events in the coming year.[3] Most also reported experiencing disruptions over the past year—from operational shutdowns and productivity losses to supply chain failures, higher expenses, and property damage.[4]

Audit committees should engage management as to how they're identifying, monitoring and mitigating the risks facing the organization and whether they have the capabilities within their teams to do so. In addition to monitoring incidents, organizations should run climate and cyber scenarios to stress test the organization's resilience to events such as extreme weather clusters or AI-enabled attack patterns and use predictive analytics to identify vulnerabilities across the organization. Audit committees should also engage management to ensure controls restrict use of unapproved AI tools on work devices and require attestations to use only authorized solutions.

Innovation oversight: balancing opportunity and risk

AI adoption is widespread—78 per cent of Canadian CEOs cite it as a top investment priority—primarily to improve their organization's productivity.[5] Yet risk assessments often focus narrowly on AI models.

Audit committees should ensure that management also evaluates risks from integrating AI into existing processes, such as data protection, privacy and copyright concerns. Internal controls and compliance measures must adapt to reflect AI's impact on risk profiles. Alarmingly, 42 per cent of employees report uncertainty about whether their organizations have AI controls in place, a slight increase from the previous year.[6] This highlights the need for stronger governance and employee awareness regarding AI use and risk management.

AI is increasingly being leveraged in cybercrime to attack organizations. Nearly nine in 10 Canadian business leaders in a KPMG survey named cyberattacks the greatest threat to their three-year growth plans, and 83 per cent expressed concerned that they can't withstand current, let alone, next-generation cyberattacks.[7]

As the pace of innovation accelerates and new business models and products are adopted, audit committees would be required to oversee how organizations assess both the immediate and secondary effects of these technologies. For example, the rise in usage of digital assets such as stablecoins can impact organizations through market volatility and funding costs. With the cost of capital increasing, audit committees should critically engage management's understanding of risks associated with the adoption of emerging technologies and their potential impact on the resiliency and financial health of the organization. Given the rise of AI-enabled cyberattacks, committees should encourage predictive threat monitoring and routine tabletop exercises simulating next-generation attacks to validate detection, response, and recovery.

Building organizational capability for effective risk management

Managing today's interconnected risks requires robust capabilities across all three lines of defense: business lines, risk and compliance, and internal audit. Audit committees should engage management to ensure that the right skillsets exist within the organization, usage of advanced

[3] KPMG in Canada. "Canadian leaders ramp up weather emergency readiness amid wildfire woes". Accessed November 4, 2025.
[4] KPMG in Canada. "Leadership in the breach". Accessed October 20, 2025.
[5] KPMG in Canada. "Leadership in the breach". Accessed October 20, 2025.
[6] KPMG in Canada. "GenAI adoption index".
[7] KPMG in Canada. "Canadian businesses call for government 'cyber firefighters' amid escalating threats". Accessed November 4, 2025.

technologies to bolster the risk management capabilities, employees receive adequate training to identify, manage emerging risks and that risk management functions are properly resourced. Audit committees may be required to recruit or upskill members with expertise in areas like AI, cybersecurity, climate risk, and geopolitical analysis. Financial competence remains critical but evolving risks demand a broader set of skills for audit committee members, including understanding technologies and associated risks and how these risks might manifest into potential issues for the enterprise.

> Audit committees must connect the dots between the algorithm, the hurricane and the trade dispute. True oversight now means rigorously questioning how the company anticipates, absorbs and adapts to the shocks of tomorrow.

Jas Hothi
Partner, Risk Consulting Financial Services, KPMG in Canada

Envolving governance for a dynamic risk environment

To keep pace with the rapidly changing risk landscape, audit committees may need to consider moving beyond traditional quarterly meetings. More frequent information sharing and "deep dives" into emerging issues can help organizations remain proactive. For instance, real-time monitoring of resilience indicators—such as supplier risk concentration, IT recovery capabilities, and third-party dependencies—is vital. Committees should ensure management maintains a risk-ranked inventory of critical services and promptly communicates material concerns.

By evolving their own practices, audit committees can guide organizations through turbulent times. Pairing resilience with a disciplined productivity agenda ensures performance gains are sustainable, transparent, and aligned with long-term goals, helping organizations not just survive disruption, but thrive.

Contact us

Akber Merchant
Partner, Regulatory and Risk Advisory (RRA)
KPMG in Canada
akbermerchant@kpmg.ca

Jas Hothi
Partner, Risk Consulting Financial Services
KPMG in Canada
jashothi@kpmg.ca

kpmg.com/ca/audit