AI risks and opportunities are at the heart of the audit committee agenda

With AI's growing importance and rapid deployment, audit committees should be addressing its governance and risk management.

Every audit committee needs to be thinking about AI. Its pace of innovation, rate of adoption, impacts on productivity, and pervasiveness make it impossible to ignore. According to our recent CEO Outlook survey, understanding and implementing generative AI across the enterprise is the top operational priority for organizations to achieve their growth objectives over the next three years.[1] Agentic AI—which can perform tasks with limited human intervention—is increasingly being adopted by organizations, with 86 per cent of business leaders citing agentic AI as a top investment priority for their organization.[2] This is affecting processes, systems and controls across the organization and how humans are being kept in the loop. As such, AI should be on the agenda of audit committees, whether their mandate involves oversight of risk management for the broader organization or entails a more traditional focus on the financial function.

> AI has great potential to increase the efficiency and productivity of organizations and remain competitive in global markets, so audit committees must carefully weigh the mitigation of risks against the potential to stifle the organization's competitiveness.

Stephanie Terrill
Canadian Managing Partner, Digital and Transformation and National Leader, Management Consulting, KPMG in Canada

> 62% of employees surveyed use publicly available tools, while 28% use enterprise versions—yet 91% of leaders are concerned about sensitive information going into public tools.[3]

Audit committees must understand where and how AI is being used

Audit committees need to understand where and how AI is being used in the financial reporting process and what the associated risks are. Depending on their mandate, some committees may also need to ask about its use across the entire organization. Regardless of the committee's scope, this inventory should include

[1] KPMG in Canada. "Productivity in the deep". Accessed October 21, 2025.
[2] KPMG in Canada. "Canadian organizations turning to AI agents: KPMG poll". Accessed November 7, 2025.
[3] KPMG in Canada. "Generative AI Adoption Index 2025." Accessed November 28, 2025.

AI in applications that are under development and AI that is being introduced through upgrades to technologies that are already in use.

Organizations should also ensure that employees are not using unauthorized AI-driven tools, which may not be suitable for the organization or the task to which they're being applied— this could produce inappropriate results, increase cybersecurity risk, and compromise data security, data privacy, and competitive advantages.

Organizations may wish to strengthen their IT governance by encouraging the use of authorized AI-driven tools in ways that align with employees' roles and responsibilities. As part of a broader risk management strategy, some organizations are exploring measures such as employee attestations and technical controls to help ensure that only approved, compliant AI solutions are accessible on work-issued devices. This approach can help foster a secure and well-managed environment for AI adoption, while supporting organizational objectives and compliance needs.

To build on these governance measures, it is equally important for audit committees to engage management in discussions about the suitability and oversight of AI tools in practice. Management should be questioned about how they're ensuring AI tools are fit for purpose and that their output is appropriate from accounting and ethical standpoints. For instance, tools affecting people—such as those used in the recruitment process—are vulnerable to bias that should be monitored and corrected. As most of these tools are new, human oversight and judgement should still be applied to the results and modifications should be made to tools where errors occur. Management should demonstrate to the committee that they have robust controls in place to manage potential risks from these tools and from the changes to existing systems and processes arising from the integration of AI.

Questions audit committees should be asking:

- Where is AI being used in the organization today?
- Does our organization have an AI policy that covers AI governance, AI data security and privacy, and AI training and education?
- Does our board have digital or AI skills to effectively govern?
- What is our general framework for governing the use of AI?
- How are we educating our workforce on AI risks, policies and proper use?
- How are we evaluating and monitoring third-party risk as we bring on new AI-related vendors and vendors that use AI?
- How is AI affecting the external auditor through their use of it and our use of it?
- How are we ensuring proper data management and protection as we use more AI?

71% of business leaders rank data quality as the top factor for AI-driven growth. However, nearly half (49%) of employees have seen inaccurate or biased AI outputs; 58% are very/extremely concerned about hallucinations; 46% say this holds them back, and 37% avoid tools because fact-checking adds work.[4]

Examining how AI is affecting the external auditor

To ensure comprehensive oversight of AI-related risks and opportunities, audit committees should also look beyond the organization's internal practices and consider how external parties—such as auditors—are engaging with AI. The audit committee should ask the external auditor how it uses and governs AI in its practice and how its work is affected by the organization's use of AI—focusing on explainability rather than accepting "black box" outputs. For example, the committee can probe how the auditor evaluates supporting evidence generated with AI by requiring the auditor to explain the model's purpose, inputs, data provenance, assumptions, and limitations, and to demonstrate how results are validated and subjected to human oversight. The committee should also confirm that the auditor is educating and training its workforce on explainability, responsible AI use, and the organization's AI policies to ensure ongoing competency.

AI can add new dimensions to old risks

AI has the potential to introduce new challenges to cybersecurity, so efforts to protect corporate data and personal information should be paramount. For instance, some AI applications involve off-site storage and processing of data. The audit committee should ensure management is adapting cybersecurity and data privacy practices to account for the use of AI. Management should know where the organization's data is stored and, if it leaves the organization's boundaries, they should be evaluating the security of this off-site storage on an ongoing basis. Management should also determine whether any third-party AI vendor is using the organization's data to train or fine-tune its models, under what data-sharing terms, and with what safeguards, and ensure these practices align with the organization's privacy, security, and intellectual property requirements.

In general, third-party risk related to AI is increasing. Existing large technology companies are integrating AI into their products, many new vendors are offering AI solutions and many non-technology vendors are using it in their operations. The audit committee should question management about how they're vetting new AI-related vendors and monitoring AI use in third parties' operations. The risk profile and competitive position of organizations will continue to evolve as AI is adopted across the industry.

> AI now affects all organizations, and it belongs on every audit committee agenda. Committees must address its governance, risk management and impact on financial reporting.

Bryant Ramdoo
National Audit and Assurance Innovation Leader, KPMG in Canada

[4] KPMG in Canada. "Generative AI Adoption Index 2025." Accessed November 28, 2025.

Regulators are monitoring AI

Most jurisdictions and securities regulators are examining regulations and reporting requirements for AI but, so far, few have issued formal requirements. The EU Artificial Intelligence Act came into force on August 1, 2024. It prohibits certain AI uses and regulates others according to their level of risk by mandating requirements for such items as risk management, data governance, record-keeping and documentation, and human oversight.

The Securities and Exchange Commission (SEC) has not issued a final rule on AI but expects disclosures of related material risks and events within existing reporting frameworks—and has cautioned companies about misrepresenting their use of AI. In Canada, the federal government has released a voluntary code of conduct for advanced generative AI systems, while the Canadian Securities Administrators (CSA) has released a staff letter that doesn't create any new requirements but provides guidance on applying existing securities laws to AI. Audit committees will need to ensure management stays apprised of regulatory changes and, where required, is compliant.

The Canadian Public Accountability Board (CPAB) has also put out a report on the use of AI in the audit. It advises "balancing innovation and risk," which is a sentiment that highlights the difficult balancing act that boards, audit committees and management face when governing AI in the organization.[5] AI brings with it many risks that must be mitigated, but fear of this risk must not stifle the opportunity that AI brings.

AI governance begins with a general framework

It will be challenging for governance to be adapted to every innovation or implementation of AI, but a well-designed foundational framework of general policies regarding the use of AI can provide adequate risk assessment and governance—while being generic enough to offer guidance through different iterations.

AI literacy should be a central tenet of this framework and evidence suggests that there's room to improve this at Canadian organizations. Canada ranks 44th out of 47 countries in AI literacy; only 24 per cent of Canadian respondents say they've received training in AI; and fewer than half (47 per cent) believe they can effectively use AI tools, according to the KPMG International and University of Melbourne research report *Trust, attitudes and use of artificial intelligence: A global study 2025*.[6]

> 83% of employees want to upskill; 82% want employer-provided training—but only ~48% feel they get sufficient training.[7]

AI education is essential

AI education must move beyond training on how to use a tool and be tailored to the different functions and risk profiles in the organization. This education should include training on the risk of AI and the company's policies around its appropriate and effective use, as well as discussions of how using AI can contribute to larger business objectives. It should also be

[5] Canadian Public Accountability Board. "The use of artificial intelligence in the audit — balancing innovation and risk". Accessed October 29, 2025.
[6] KPMG in Canada. "Canada is lagging behind global peers in AI trust and literacy". Accessed November 7, 2025.
[7] KPMG in Canada. "Generative AI Adoption Index 2025." Accessed November 28, 2025.

tailored to different functional areas, which will have access to unique types of data. This will require different uses of the same tools and specific procedures and precautions around the optimal use of these tools.

To properly oversee AI within the organization, audit committees should ask management how they're educating themselves and their employees on AI and how they're monitoring its effectiveness. They should also evaluate their own level of knowledge and determine whether they may need additional education or even consider recruiting to bolster their AI literacy.

The ubiquity of AI demands attention, and this begins with understanding it.

Contact us

Stephanie Terrill

Canadian Managing Partner,
Digital and Transformation and National Leader, Management Consulting
KPMG in Canada
sterrill@kpmg.ca

Bryant Ramdoo

National Audit and Assurance Innovation Leader
KPMG in Canada
bramdoo@kpmg.ca

kpmg.com/ca/audit