AI Transformation: Audit Committees play a crucial role

Audit committees bring insight into people processes and risks to AI transformation

By Andrew Forde

While AI transformation is a part of the larger digital change, it's taking on a life of its own. Just because a company can adapt to digital doesn't mean it's ready for AI; it's a different game. There are many more considerations, and it requires a different approach. AI will change how we think—not just how we work.

While many people are excited about the possibilities of artificial intelligence, audit committees need to think bigger. As we see more advances like generative AI and powerful language models, they will need to look at data quality, rethink how intellectual property is viewed, understand stakeholder impacts, and prepare for upcoming regulations.

The emergence of AI models in various industries has led to a growing need for company boards to understand how to properly integrate, oversee and optimize these technologies within the organization. Boards must understand AI to align these models' use with the company's core objectives and ensure that AI initiatives create value and competitive advantage.

Understanding AI models is pivotal to assessing their ethical ramifications and potential biases and ensuring compliance with evolving regulations and standards, which can significantly impact corporate reputation and stakeholder relations. Audit committees must act as guardians in this rapidly evolving AI landscape, ensuring strategic value, ethical integration and organizational resilience.

Bringing AI to the enterprise is complex

Companies should think carefully before implementing AI solutions– and particularly GenAI. Transferring the intended benefits of AI proofs of concept (PoC) to enterprise-ready products or services is challenging. PoCs are obtained in highly structured environments where the input data has been sanitized, ensuring the model behaves as intended. When released into the organization where things are not perfectly curated, the model might not perform as expected or it may access data it wasn't meant to.

> By acting as guardians of the broader concerns around AI, audit committees will foster trust and transparency and enhance the credibility of AI technologies in ways that influence people, businesses, and society.

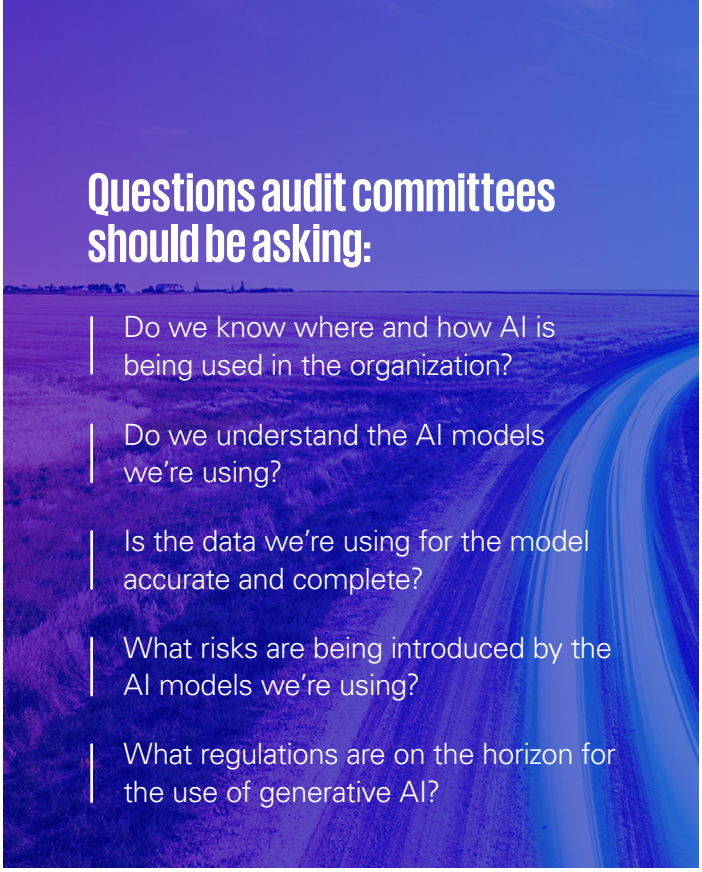
Andrew Forde
Partner, Technology Strategy and Digital Transformation
KPMG in Canada

To mitigate this, audit committees should ask management about the expected benefits of each instance of AI versus the costs and risks it might introduce. Just because something can be done using AI doesn't always mean it should be done using AI. Audit committees should request external reviews of their organizations' models regularly. They should ask management whether the applications are performing as expected, if they're only using the data they're intended to and what risk controls are being put in place around unintended outcomes.

Organizations applying AI solutions also need a proper foundation across talent, processes and data. This begins with identifying where it makes the most sense to use AI in the business and overlaying where there is enough data with the quality necessary to operationalize it. Ensuring there's executive buy-in is a must since it will require a significant commitment of time and resources.

With any new model adoption, the audit committee will need to take a leadership role in driving conversations with management around cyber security, data privacy and regulatory compliance, and how models will interact with other applications the organization uses. They will want to ensure that potential risks are mitigated through appropriate processes and controls and that the firm is engaging the right talent for AI initiatives.

Most organizations will not build AI solutions from scratch. Instead, they will buy applications that already have AI models built into them. Where this is the case, the audit committee will need to understand the risks introduced by these solutions, the controls put in place by the vendor and how these measure up to the control standards of the organization.



Human impact is shaping adoption and driving regulation

The most important concern about AI is its impact on people. Although it offers many potential positive implications for humans, AI may also negatively impact such things as privacy, health, economic security and justice. The materiality of these negative impacts will govern the application of AI and its regulation.

The materiality discussion will likely begin around security and privacy. Then, depending on the industry, it will consider the human impact such as changing or eliminating job roles or recommending medical treatments. As these impacts become more material, transparency and documentation will be imperative.

Audit committees will need to ask questions about biases in the models and how processes are being documented. They will also need assurances from management that, at any given time, they can validate that the models are doing what they're supposed to do, that there's no misuse of data and that customers can be confident that the proper measures are in place to ensure there's no downside risk to engaging with the organization.

The materiality of human impact is already shaping which AI applications are being implemented in the enterprise. It's being used most often for batch processes in the back office and for making personalized product or service recommendations because these have a low impact on people, which reduces the potential compliance and regulatory burden that might accompany their growth.

That said, as concerns grow about human impact, regulation is likely to accelerate progress in the commercial use of AI–which seems counterintuitive. Generally, regulation is seen as an inhibitor of innovation or adoption. However, AI regulatory oversight will help companies build trust and confidence with the public and allow greater use of AI by the company. Regulated organizations will be able to assure the public that they have a risk management framework in place that is tracked and validated by third parties.

Regulations will ramp up quickly as AI produces more material impacts for people. The Canadian government has recently issued draft guidelines that some organizations have adopted voluntarily and discussions are taking place within industries such as healthcare as to what certification would look like [1]. These regulations will surely change and evolve before becoming mandatory for anyone using materially impactful models. Still, audit committees should get ahead and prepare their organizations for what's to come.

We will think differently about IP

One concern about generative AI is that it's using data that some consider proprietary intellectual property (IP) through data gathering techniques such as scraping the internet. There's also concern about which databases and even personal information may become accessible. However, we've seen with mobile phones that if people are getting benefits, they're less concerned with what happens to their data. The same is likely to occur with organizations and their IP.

The way we view IP will change. From the Industrial Revolution to today, we've been an economy of specialists. We're now seeing a shift where specialization has less value—because computers have access to all data all the time and can synthesize

[1] "Minister Champagne launches voluntary code of conduct relating to advanced generative AI systems," Montreal, September 27, 2023, https://www.canada.ca/en/innovation-science-economic-development/news/2023/09/minister-champagne-launches-voluntary-code-of-conduct-relating-to-advanced-generative-ai-systems.html

it at incomprehensible speeds. As a result, IP will be centred more around the architecture of systems of people, processes and technology, and bringing these together to reach desired outcomes. As this happens, data will become more democratized with more sharing of what we consider IP today.

This democratization of IP will have implications for almost all aspects of the business, from processes to talent and even the makeup of the audit committee itself. While it's not imminent, audit committees must watch for changes in how information is treated and assess the implications for controls, processes, data and reporting.

The assurance expertise of audit committees will initially allow them to provide valuable oversight of AI without needing in-depth knowledge of it. They will want to ask management about the nature and magnitude of risks being introduced through the AI applications being used, as well as cyber security, data integrity and quality, and the costs and benefits of using AI tools. They may wish to consult outside experts if deeper technical insight is required. As AI adoption grows, their own expertise will grow but they may need upskilling or committees will have to recruit new members with specialized AI knowledge.

As a starting point, audit committees should begin requesting a "corporate report on AI" detailing the integration, use and impact of artificial intelligence within the organization. It should scrutinize the alignment of AI with corporate strategy, evaluate risk management pertaining to AI applications, and assess the ethical implications and compliance with relevant regulations. It should meticulously review AI initiatives, their efficacy and ROI and offer strategic recommendations for enhancing operational efficiency and competitive advantage. This report will facilitate informed decision-making and ensure the responsible and optimal deployment of AI, paramount for sustaining corporate integrity, mitigating risks, and fostering innovation.

Applying AI tools to the enterprise brings complexities and risks. Audit committees bring valuable oversight and guidance to this technological evolution through their understanding of risk and assurance.

Contact us

Andrew Forde
Partner, Technology Strategy,
and Digital Transformation
KPMG in Canada
416-468-6968
andrewforde@kpmg.ca