Acceleration of AI ups the ante on governance

KPMG Board Leadership Centre

Rapid advancements in artificial intelligence (AI) and the implications for governance and board oversight are front and centre.

The era of AI has begun with startling speed. AI and machine learning are increasingly driving business decisions and activities, and pressures continue to mount – from customers, regulators, and other stakeholders – for greater transparency into how these data-driven technologies and algorithms are being used, monitored, and managed. In particular, they want to understand how companies are addressing the risks associated with AI systems – risks such as algorithmic biases in healthcare scoring and access to healthcare services; job application vetting and recruiting and hiring practices; loan credit decisions; privacy violations; cybersecurity; disinformation and deepfakes; worker monitoring; and more recently, the risks posed by generative AI.

Despite the explosive growth in the use of AI systems and increasing concerns about the risks these systems pose, many organisations have yet to implement robust AI governance processes. In a recent global survey of more than 1,000 executives by BCG and *MIT Sloan Management Review*, an overwhelming majority (84 percent) said that responsible AI should be a top management priority. Yet, just 16 percent of their companies have mature programs for achieving that goal.[1] Notably, a recent KPMG survey found that relatively few C-suite executives are directly involved in, or responsible for, strategies to manage AI risk and data/model governance, including establishing new processes or procedures (44 percent), reviewing AI risks (23 percent), and developing and/or implementing governance to mitigate AI risk (33 percent).[2]

Given the legal and reputational risks posed by AI, many companies may need to take a more rigorous approach to AI governance, including (i) monitoring and complying with the patchwork of rapidly evolving AI legislation, (ii) implementing emerging AI risk management frameworks, (iii) securing AI pipelines against adversarial threats; and (iv) assessing their AI governance structure and practices to embed the guardrails, culture, and compliance practices that will help drive trust and transparency in tandem with the transformational benefits of AI. The goal is often referred to as "ethical" or "responsible" AI – that is, making AI systems transparent, fair, secure, and inclusive. Below, we offer comments on these four areas of board focus.

Monitoring and complying with evolving AI legislation

In addition to general data privacy laws and regulations, we are now seeing the emergence of AI-specific laws, regulations, and frameworks globally. For example, the EU's Artificial Intelligence Act appears to be on the path to becoming law, perhaps by the end of 2023. The act may set a precedent for future risk-based regulatory approaches, as it would rank AI systems according to their risk levels, and ban or regulate AI systems based on those risk levels.

There is no similar legislative framework in the UK and the UK Government have announced that they wish to avoid heavy-handed legislation that could stifle innovation, choosing instead to empower existing regulators to prepare tailored, context-specific approaches that suit how AI is used in each specific sector.

[1] Elizabeth M. Renieris, David Kiron, and Steven Mills, "To Be a Responsible AI Leader, Focus on Being Responsible," MIT Sloan Management Review and Boston Consulting Group, September 2022

[2] Responsible AI and the Challenge of AI Risk, 2023 KPMG U.S. AI Risk Survey Report

This approach to regulating AI – which is intended to build public trust and make it easier for businesses to grow and create jobs – is set out in the March 2023 white paper A pro-innovation approach to AI regulation.

Monitoring and complying with evolving AI legislation and regulation will be a key priority for companies over the next year.

Eight core principles to guide responsible AI

1. Fairness
Ensure models are equitable and free from bias. AI should not discriminate against individuals or create unfair outcomes.

2. Explainability
Ensure AI can be understood, documented, and open for review. Organisations developing and deploying AI should be able to communicate when and how it is used and explain a system's decision-making process in an appropriate level of detail that matches the risks posed by the use of the AI**.**

3. Accountability
Ensure mechanisms are in place to drive responsibility across the lifecycle. Measures are needed to ensure there is appropriate oversight of the way AI is being used and clear accountability for the outcomes.

4. Security
Safeguard against unauthorised access, corruption, or attacks. AI should function in a secure, safe and robust way where risks are carefully managed.

5. Privacy
Ensure compliance with data privacy regulations and consumer data usage e.g., the UK General Data Protection Regulation.

6. Safety
Ensure AI does not negatively impact humans, property, or the environment.

7. Data integrity
Ensure data quality, governance, and enrichment steps embed trust.

8. Reliability and redress
Ensure AI systems perform at the desired level of precision and consistency. People need to have clear routes to dispute harmful outcomes or decisions generated by AI.

Implementing emerging AI risk management frameworks

AI risk management has been a particular challenge for many companies, and the potential use of generative AI has now created a sense of urgency. While there are various standards and best practices to help organisations manage the risks of traditional software or information-based systems, the risks posed by AI systems present new challenges. To help companies address these challenges, in January, the US National Institute of Standards and Technology (NIST) published its AI Risk Management Framework, which is intended for voluntary use to help organisations address risks in the design, development, deployment and use of AI systems, and evaluation of AI systems to increase the trustworthiness of AI systems. Given the critical importance of AI risk management, boards should have their management teams assess whether the AI Framework can provide helpful guidance in building or enhancing the company's AI risk management structure and processes.

Securing AI pipelines against adversarial threats

Given the current AI arms race, companies need to have processes in place for securing and hardening AI pipelines against adversarial threats. In addition to ethical and bias considerations that may inadvertently come from developing AI systems, consider the threats and impacts from adversarial attacks, including data poisoning, model poisoning, back doors, insider threats, and other ways that attackers might damage the company's decision-making systems. Indications are that adversaries are arming themselves with tools to attack AI systems and profit from a lack of humans in the loop. Frameworks like MITRE ATLAS identify threats and mitigations that can be leveraged to better prepare the organisation for these attacks.

Assessing AI governance structure and processes

Delivering on the promises of AI while managing the risks requires robust AI governance structures and processes, aligned with the company's broader risk management, data governance, and cybersecurity governance processes.

To this end, in addition to the topics discussed above, we recommend that boards discuss with management the following issues:

- The need for (or adequacy of) a cross-functional management steering committee to establish policies and guidelines regarding the company's development, use, and protection of AI systems and models. How and when is an AI system or model – including the use of third-party generative AI services – to be developed and deployed, and who makes that decision? Benchmark the role, composition, and policies of such a steering committee against industry best practices.
- What AI systems and processes has the company deployed, and which are the most critical?
- What regulatory compliance and reputational risks – including biases – are posed by the company's use of AI? How is management mitigating these risks?
- How is management coordinating its AI governance activities with its cybersecurity and broader data governance activities?
- Does the organisation have the necessary AI related talent and resources?
- Are the company's AI systems transparent, fair, secure, and inclusive – i.e., ethical and responsible – and consistent with the company's purpose, values, and sustainability commitments?
- Are the broad, potentially game-changing implications of AI – for the company's industry, business model, and long-term viability and competitiveness – being factored into strategy discussions?

The KPMG Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. Membership offers you a place within a community of board-level peers with access to topical and relevant seminars, invaluable resources and thought leadership, as well as lively and engaging networking opportunities. We equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Learn more at www.kpmg.com/uk/blc.

Contact us

Timothy Copnell

Board Leadership Centre

T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk

www.kpmg.com/uk/blc

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.