KPMG

# Oversight of data-related risks

## From data governance to GenAI and cybersecurity

KPMG Board Leadership Centre

**While data governance has been a priority for companies for some time, the explosive growth in the use of generative artificial intelligence (GenAI) has emphasised the importance of data quality, having a responsible use AI policy, complying with evolving privacy and AI laws and regulations, and rigorously assessing data governance practices.**

Given the strategic importance of data to a company—and the increased focus by customers, investors, and regulators on data-related risks and how a company uses and protects data—boards should probe whether the company's data governance framework and interrelated AI, GenAI, and cybersecurity governance frameworks are keeping pace.

Below we discuss four key areas for board focus:

- The adequacy of the company's data governance framework.
- Elements of a governance framework for AI and GenAI.
- How management is enhancing cybersecurity risk management processes to address the risks posed by AI and GenAI.
- Structuring board and committee oversight of these issues.

## Adequacy of the data governance framework

- Companies typically develop their data governance framework based on their industry and company-specific facts and circumstances. Frameworks vary in many respects, but generally focus on four pillars: data quality, data stewardship, data protection and compliance (or privacy and security), and data management. While a detailed review of these pillars is beyond the scope of this paper, key elements of a data governance framework include:
- **Alignment with strategy**. Does the framework support the company's current strategy? Is there alignment across the C-suite on the company's data governance priorities? Which of the company's strategic goals are dependent upon data?
- **Structure of data governance program**. How is the data governance program structured from an operational point of view? For example, has management created a data governance council? Clarify which business leaders are responsible for data governance. Recognising that companies may have several executive officers with differing responsibilities for data governance, what is the role of each of the executive officers—e.g., the chief data officer, chief information officer (CIO), chief information security officer (CISO), and chief compliance officer? Who has overall responsibility, and who does that individual report to? Does management have the people, skills, training, technology and other resources (including internal funding) to effectively manage data?
- **Compliance with data privacy laws and regulations**. In addition to industry-specific laws and regulations, several privacy laws and regulations govern how personal data—from customers, employees, or vendors—is processed, stored, collected, and used, and grant consumers certain rights regarding their data. Examples include the EU General Data Protection Regulation and the California Consumer Privacy Act. Global and domestic laws and regulations place a substantial compliance burden on companies, and violation of some of these laws and regulations can result in substantial penalties.
- **Data ethics**. Beyond technical compliance, companies need to manage the tension between how they use customer data in a legally permissible way with customer expectations (for example, to protect the personal privacy of individuals). This tension poses significant reputational and trust risks for companies and represents a critical challenge for leadership.
- **Data hygiene**. Does the company limit data collection and storage to only data that is necessary to support its strategy?
- **Access**. Which vendors and third parties have access to company data? Do they have controls in place to manage the data in accordance with the company's policies? Does data received from third parties comply with agreements between those parties and the company? As to highly sensitive data, who should have internal access? Who is verifying compliance?

- **Internal audit**. Does internal audit review the data governance program to identify risks and assess compliance with processes and procedures?
- **Third-party assessment**. Should the data governance framework and program be reviewed by a third party?
- **Culture of data governance**. How does management ensure adoption and compliance with data governance practices and policies throughout the company?

Directors should understand the company's data-related risks, their magnitude, who is managing those risks, and the downside scenarios. Is the board briefed on data risks associated with the company's use of data, including data quality, security, privacy, and regulatory compliance? How are those risks proactively or retrospectively addressed from people, process, and technology perspectives? How often is management's risk assessment updated?

## Elements of an AI / GenAI governance framework

With AI and GenAI increasingly driving business decisions and activities, customers, regulators, and other stakeholders are seeking greater transparency into how these data-driven technologies and underlying algorithms are used, monitored, and managed. They want to understand how companies are addressing the risks posed by AI and GenAI systems—such as risks associated with 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; and worker monitoring.

Embedding guardrails, culture, and compliance practices can help companies 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.

### Monitoring and complying with evolving AI legislation

We are seeing the emergence of AI-specific laws and regulations at both local and global level. For example, in March, the European Parliament passed the European Union AI Act, the first comprehensive attempt to regulate AI globally.

The AI Act became effective across all EU Member States on 1 August 2024, and the enforcement of many of its provisions will commence in August 2026. The AI Act generally adopts a risk-based approach to the deployment and use of AI systems. Furthermore, the Act has broad, extraterritorial reach, and covers any entity that is "placing on the market" or "putting into service" an AI system in the EU.

Also, the Act provides for significant penalties for violations, making it important for companies to carefully evaluate whether they are subject to the legislation, and if so, whether their practices, services, and products are compliant. Companies should consider benchmarking against the AI Act since other regulators may look to it when considering potential regulation.

There is no similar legislative framework in the United States; however, in October 2023, President Biden signed an executive order on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which could be the basis for future legislation/regulation. Several other countries are also developing AI principles and frameworks. Monitoring and complying with evolving legislation and regulation should be a priority.

### Implementing emerging AI and GenAI risk management frameworks

One of the overarching risks posed by GenAI is reputational risk. Trust and reputation, as well as alignment with the company's values and mission, are critical factors when considering how GenAI will be developed and deployed. Companies should develop a responsible-use policy to manage the risks that GenAI may pose to individuals, organisations, and society.

While there are various standards and best practices to help companies manage the risks of traditional software or information-based systems, the risks posed by AI systems present new challenges. However, AI and GenAI risk management frameworks are emerging – for example, the National Institute of Standards and Technology's (NIST's) AI Risk Management Framework (AI RMF), which is intended for voluntary use to help organisations address risks in the design, development, deployment, use, and evaluation of AI systems to increase their trustworthiness. Given the critical importance of AI risk management, boards should have their management teams assess whether the AI RMF can provide helpful guidance in building or enhancing the company's responsible use policy and should also consider whether the company's Code of Conduct should be updated accordingly.

### Adopting data quality leading practices

Achieving the hoped-for productivity and efficiency improvements with AI and GenAI will depend on the quality of the company's data and how it is processed and stored. The quality and accuracy of the company's data, and how it differs from competitors' data, will be critical to competitive advantage. Boards need insight into whether companies are making the right investments in IT infrastructure and data quality to ensure that the company's AI and GenAI output is accurate.

### Assessing AI / GenAI governance structures and processes

Delivering on the promises of AI and GenAI while managing the risks requires robust governance structures and processes aligned with the company's broader risk management, data governance, and cybersecurity governance processes. Boards should consider discussing the following questions with management:

- How is an AI or GenAI system or model—including third-party GenAI services—developed and deployed, and who makes that decision? Is there cross-functional management steering committee to establish policies and guidelines regarding the company's development, use, and protection of AI and GenAI systems and models?

- Is there a complete and current inventory of the AI and GenAI systems, processes, and uses the company has deployed?
- How is management identifying and mitigating the risks posed by AI and GenAI and ensuring that the use of AI and GenAI is aligned with the company's values? What AI and GenAI risk management frameworks are used? How frequently are risk assessments updated to reflect changes in the technology and business environment? Are the results shared with the board?
- How is management monitoring rapidly evolving AI and GenAI legislation, and ensuring compliance?
- Does the organisation have the necessary AI and GenAI-related talent and resources, including in finance and internal audit, particularly given the war for talent in these areas?
- How is management coordinating its AI and Gen AI governance activities with its cybersecurity and broader data governance activities?
- Are the company's AI and GenAI systems transparent, fair, secure, and inclusive—i.e., ethical and responsible—and consistent with the company's purpose, values, and ESG/sustainability commitments?

With GenAI affecting multiple aspects of a business—strategy, risk, ethics and compliance, talent, human resources, operations, brand and reputation—a broad range of C-suite functions may have responsibility and accountability for various aspects of GenAI. This might include the CEO, general counsel, chief financial officer, chief risk officer, and chief operating officer, with a chief technology officer or CIO as the person with ultimate responsibility for GenAI. This highlights the challenges and complexity of GenAI adoption and use, as well as the need for a cross-functional management team, as well as leadership and coordination at the most senior levels of management.

## How management is enhancing cybersecurity risk management processes to address the risks posed by AI and GenAI

Many companies and their boards have devoted substantial time and resources to understanding cybersecurity risk, and making sure the company has the right governance, technology, and leadership in place to manage and mitigate the risk. In light of the growing cybersecurity risks posed by GenAI, boards should review with the CISO or other senior cybersecurity executive the steps being taken to help ensure that management's cybersecurity risk management practices are keeping pace with increasingly sophisticated threats.

GenAI can write code used to hack and to create more realistic and sophisticated deep fakes and phishing scams, substantially increasing threats and cyber risk exposure. As a result, GenAI may enable cybercriminals to scale their attacks in terms of speed, volume, and variety, heightening the risk of data breaches, malware attacks, and phishing attacks.

To counter these risks, cybersecurity teams should review their security postures, including assessing current systems, identifying vulnerabilities, and making adjustments to enhance protection as needed. The results of this review should be shared with the board.

The following considerations may also be helpful as boards refine their cybersecurity discussions:

**Periodically review management's cybersecurity risk assessment**

Every company should be conducting cybersecurity risk assessments as a matter of course. Key areas of focus should include cybersecurity leadership and governance, human factors or "people risks," legal and regulatory compliance, business continuity, operations and technology, and information risk. What are the company's most valuable digital assets and what are the greatest threats and risks to those assets? Are there security gaps? How quickly can a security breach be detected?

**Take a hard look at supply chain and other third-party risks**

Robust reporting of third-party risks—and close linkage with the company's risk management process—should be front and centre for the board. Board conversations should focus on whether the company's inventory of third parties is up to date, and whether third-party cybersecurity controls have kept pace with the changing risk environment. Most importantly, do they meet the company's own standards and contractual requirements?

**Insist on a cybersecurity scorecard**

Many audit committees and boards discuss with management a cybersecurity scorecard for the most recent period, including the volume of cyber incidents, the materiality and nature of cyber incidents and how they are being managed, and trends and developments in the external environment. A cybersecurity scorecard can help improve the quality of cyber information and the quality of director dialogue regarding cybersecurity.

**Understand and periodically reassess the company's cyber incident response plan**

Companies need to ensure that their cyber incident response plans, policies and procedures keep pace with the evolving cyber risk landscape.

In the US, the SEC have adopted final rules that require public companies to disclose material "cybersecurity incidents" within four business days of a materiality determination. The SEC final rules also require companies to disclose detailed information regarding their cybersecurity risk management strategy, and governance.

## Structuring board oversight

For many companies, much of the board's oversight responsibility for cybersecurity and data governance has resided with the audit committee. In our 2023 Audit Committee Survey, 70 percent of respondents reported that their audit committee had significant oversight responsibilities for data governance, and 62 percent for cybersecurity.

In addition, 80 percent of respondents reported that their audit committee had significant oversight responsibilities for legal/regulatory compliance, which includes compliance with evolving data privacy and AI-specific laws and regulations globally.

Given the audit committee's heavy agenda, it may be helpful to consider whether another board committee should monitor and do some of the heavy lifting related to cybersecurity, data governance, and other tech issues. Does another board committee(s) have the time, composition, and skill set to oversee these issues? Is there a need for an additional committee, such as a technology or risk committee? If cybersecurity and data governance oversight are assigned to a technology or other committee, the audit committee would still have some oversight responsibilities in these areas (e.g., oversight of internal and disclosure controls and procedures).

Many boards are still considering how best to oversee AI and GenAI and the appropriate roles of standing committees as they seek to understand GenAI's potential impact on strategy and the business model. For most companies, oversight currently is largely at the full board level—where major issues typically should be discussed. Oversight structures will likely evolve as companies' GenAI programs evolve. Ultimately, oversight of GenAI, like oversight of sustainability, may touch all or most board committees, but boards should be cautious about adding to the audit committee's oversight responsibilities.

However, some board committees, such as the audit committee or a technology committee, may already be involved in overseeing specific GenAI issues. Some of the GenAI-related issues that audit committees may have oversight responsibilities for include:

- Use in the preparation and audit of financial statements and other regulatory filings.
- Use by internal audit and the finance organisation, and whether those functions have the necessary talent and skill sets.
- Development and maintenance of internal controls and disclosure controls and procedures related to GenAI.
- Oversight of compliance with laws and regulations.
- Cybersecurity and data privacy risks associated with the use of GenAI.

Data is an increasingly critical and valuable asset for almost every company, requiring a more rigorous governance approach. Oversight of data governance, AI, GenAI, and cybersecurity, and helping to develop and maintain a more exacting governance structure and approach around these areas should be a board priority.

## 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)7801 520802
**E:** tim.copnell@kpmg.co.uk

**www.kpmg.com/uk/blc**