

# — TONE — at the — TOP<sup>®</sup>

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 123 | June 2024

## Critical AI Governance Considerations



Emerging technologies present organizations with a wide variety of opportunities, but they can bring with them a range of new and unexpected risks. Indeed, in an Internal Audit Foundation survey of global internal audit leaders, 34% say digital disruption is one of the top five risks their organizations are facing, and 55% say it will be a top five risk in three years.<sup>1</sup>

Because many businesses are increasingly embracing one area of technology – artificial intelligence (AI) – boards and audit committees will need a greater understanding of its impact on their organizations and on their AI governance responsibilities. “As businesses expand their use of AI, especially into core business processes, the audit committee will need to understand the challenges and opportunities presented by AI to address risks related to governance and stakeholder trust,” notes the National Association of Corporate Directors (NACD).<sup>2</sup>

As AI takes center stage, its governance likely will be handled differently depending on the organization. In many cases, the audit committee will be expected to step up to a more complex, higher level of oversight, according to Emmanuel Manalo, head of internal audit at Lemonade, an insurtech company based in New York. Audit committees “are not just the gatekeepers, they are the guardians of ethical adoption and responsible governance of AI.” Audit committees may be facing new expectations driven company policies, emerging regulations, or accepted best practices from bodies such as COSO<sup>3</sup> and the National Institute of Standards and Technology.<sup>4</sup> Armed with a solid understanding of the company’s AI strategy, the audit committee will need to determine whether that strategy is aligned with the company’s overall risk appetite and goals. Other committees, and the board itself, may be called upon to take on new roles.

## A Range of Evolving Risks

Among other issues, it will be important for boards to determine whether the company has adequate controls over AI and an understanding of whether the AI strategy addresses AI's ethical use, including issues related to privacy, accountability, and potential biases. Ethical considerations in working with AI can take many forms. For example, because of the breadth of data involved, it is inevitable that some personally identifiable information could be inadvertently included where it should not be, Manalo says. Organizations can use frameworks such as the European Union's General

Data Protection Regulation (GDPR) in developing their own guidelines. The GDPR does not specifically address AI, but the European Parliament says, "there are ways to interpret, apply, and develop the data protection principles that are consistent with the beneficial uses of AI and big data."<sup>5</sup> However, problems may not immediately be clear. Data may incorporate biases that are not evident on the surface, but once it has been processed repeatedly, a prejudice against a certain group, geography, or personal circumstances may develop, Manalo explains.



The complexity and prevalence of risks also will change over time. Operational risks will rise, for example, as AI use becomes part of the company's DNA, leading to greater danger that any drop in the quality of algorithms or models or any system failure will have a significant impact as organizations place greater reliance on AI in operations and, ultimately, in decision making.

The NACD points to additional unfamiliar AI risks including:

- Shadow IT environments, in which employees use their own software or hardware without the oversight of IT

professionals or possibly without complying with company IT protocols, leaving the organization open to a range of potential threats.

- Intellectual property and other concerns related to generative AI's lack of transparency in potentially using private or copyrighted information.
- Cybersecurity risks. While organizations are well aware of dangers in this area, generative AI can make it easier for hackers to penetrate systems or write phishing emails, for example.<sup>6</sup>

## About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 245,000 global members and has awarded more than 195,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit [theiia.org](https://theiia.org).

## The IIA

1035 Greenwood Blvd.  
Suite 401  
Lake Mary, FL 32746 USA

## Complimentary Subscriptions

Visit [theiia.org/Tone](https://theiia.org/Tone) to sign up for your complimentary subscription.

## Reader Feedback

Send questions/comments to [Tone@theiia.org](mailto:Tone@theiia.org).

## Unlimited Opportunities

AI provides unlimited opportunities for organizations to enhance productivity, cost savings, and decision making and to improve fraud and risk detection and mitigation. It also can make customers happier, Manalo notes, by allowing for more customized services. Companies should also keep in mind the

## Key Considerations for Boards

Questions for boards and audit committees to consider include:

**Will we need new experts?** The requisite level of AI expertise will depend on the significance of the change that AI will have on the organization, Manalo says. "If AI strategy and use are pervasive considerations, and technical details and governance issues will be discussed in every meeting, then it will be imperative to have someone on the board or the appropriate committee with real expertise and understanding of the nuances of AI issues." If AI is not central to their strategy, companies may be able to rely on a consultant who can expand board members' understanding of AI governance concerns and return regularly to update them on new issues in this fast-evolving space.

**Which committees are responsible for AI governance?** Because the scope of AI is wide and far-reaching, organizations that have multiple board committees should give serious consideration to which – and how many – committees need to include some responsibilities for AI in their charters. The greatest danger is that committees that should have some involvement in AI governance will assume it is being handled by another group, Manalo says. This can be solved by assigning overall responsibility for AI risk and governance to one committee and delegating specific tasks – in areas including data privacy and data quality – to other committees that are best equipped to handle them.

**Will we need new committees?** Manalo's company has created a board committee on the ethical use of machine learning and AI. Other organizations may also feel the need to create new groups to address emerging AI-related issues because this field is so nuanced and touches on a wide range of areas, including cybersecurity, compliance, and data privacy, among others.

**Should we update the charters of existing committees?** This question can be answered in part by deciding if AI has driven a new level of complexity in how the organization is mitigating risks. Charters for new committees can be written from scratch, but those for existing committees should consider topics such as whether new processes will be needed and whether existing controls are sufficient. Key performance indicators also may be needed, including ones that measure model drift (i.e., the decline in a model's predictive ability based on new developments).

## Internal Auditors as Trusted Advisors

"Wherever there is a new or emerging risk, internal audit can play an advisory role on how best to address that risk, then take on assurance responsibilities" in reporting on how well risks are being addressed, according to Manalo. With newly adopted technologies, it's difficult to provide assurance when processes have not yet been established, so advisory at the outset is critical. "As companies establish an AI governance structure, internal audit can help identify risks, ensure the organization's strategies comply with existing regulations, and determine if adequate monitoring processes are in place," he says. Once processes are up and running, internal audit can determine whether controls are working as intended and the organization continues to comply with evolving regulations.

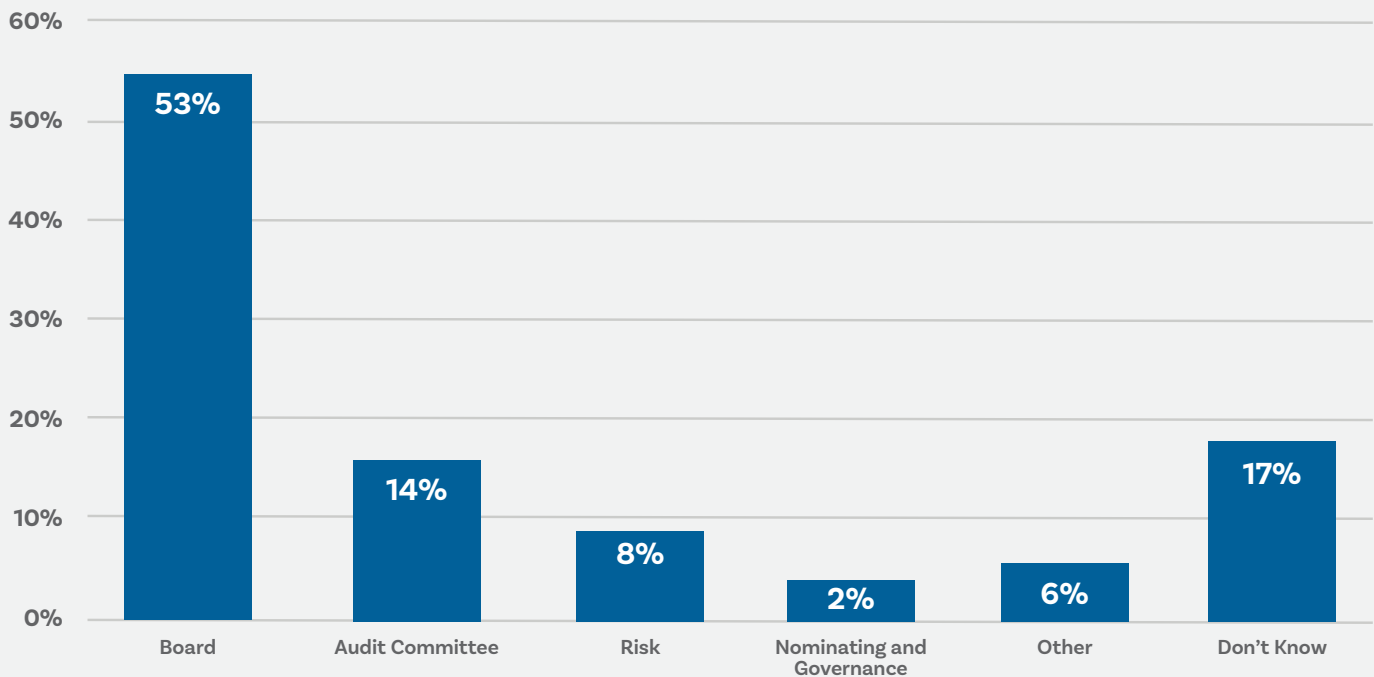
Internal audit also can help boards understand and mitigate the subtle risks that AI can bring. For example, AI can sharply enhance efficiency because it can process large volumes of data in a short time. One potential downside is that a transaction may happen before there is sufficient time for approvals to occur. Internal audit can help organizations use continuous monitoring, preventive internal controls, and backend mechanisms to enhance detection of potential fraud in this situation. Internal audit also can advise on automating data gathering, reporting, and data aggregation. "There are a lot of opportunities in terms of what internal audit can do," Manalo says.

risk of failing to implement new AI technologies. In addressing all these considerations, internal audit can be an expert partner in helping audit committees and boards cover their governance responsibilities.

## QUESTIONS FOR BOARD MEMBERS

- Does the organization have a strategy for how to use AI now and in the future?
- Does the board or any committee need greater AI expertise? Would they be best served by new members or by using expert consultants?
- Is there a holistic approach to AI governance?
- What committee or committees address AI now? Is AI governance responsibility appropriately assigned across these or other committees?

### How Is Primary Responsibility for AI Governance Divided Across the Board and Its Committees, According to Audit Committee Members?



Source: Audit Committee Practices Report: Common Threads Across Audit Committees, Deloitte's Center for Board Effectiveness and the Center for Audit Quality, March 2024.

<sup>1</sup> 2024 Risk in Focus Survey Results: Global Summary, Internal Audit Foundation, 2024.

<sup>2</sup> "Artificial Intelligence: An Emerging Oversight Responsibility for Audit Committees?", Brian Cassidy, Ryan Hittner, and Krista Parsons, NACD, December 13, 2023.

<sup>3</sup> "Realize the Full Potential of Artificial Intelligence: Applying the COSO Framework and Principles to Help Implement and Scale Artificial Intelligence," COSO and Deloitte, September 2021.

<sup>4</sup> AI Risk Management Framework and AI RMF Generative AI Profile, NIST.

<sup>5</sup> "The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence," European Parliamentary Research Service, June 2020.

<sup>6</sup> "Artificial Intelligence: An Emerging Oversight Responsibility for Audit Committees?", Brian Cassidy, Ryan Hittner, and Krista Parsons, NACD, December 13, 2023.