pwc

Governance Insights Center

June 2025

Oversight in the AI era: understanding the audit committee's role

1/3

of CEOs say GenAI has increased revenue and profitability over the past year, and half expect their investments in the technology to increase profits in the year ahead.

Source: PwC's *28th Annual Global CEO Survey,* January 2025.

57%

of directors said the full board has primary oversight of emerging tech like AI, and 17% said the audit committee has that responsibility.

Source: PwC's *2024 Annual Corporate Directors Survey,* September 2024.

For a detailed discussion of the full board's considerations, see PwC's paper:

How boards can effectively oversee AI to drive value and responsible use

Artificial intelligence (AI) is fast becoming an intrinsic part of business: strategy, growth, product innovation, operations and more. It's poised to redefine business models, revolutionize workflows and reshape entire industries.

The rapid evolution of AI is empowering companies to solve problems in unprecedented ways. Its transformative potential also reveals new avenues for growth, innovation and strategic business development.

This power does not come without risks. Realizing the full potential of AI requires understanding its risks as well as its upsides. This includes a risk management approach and appropriate policies, processes and controls to use AI responsibly in a manner that sustains trust.

The board's role in this environment is to oversee management and advise on how AI may impact strategy and risks. Typically, the full board has primary oversight of AI. Sometimes, however, the audit committee may have been given primary responsibility. In these instances, audit committee members should be mindful to focus on the strategic opportunities, not just the risks.

Even when the board has primary oversight, the audit committee has a role to play, including overseeing the use of AI in financial reporting, internal control over financial reporting, risk management and compliance. Many audit committees also oversee data security and privacy and should address the impact of AI on these areas.

A risk committee may also share oversight of AI, although only 12% of S&P 500 companies have a board-level risk committee, and those companies are primarily in financial services. For these companies, the risk committee may take on some of the responsibilities described in this paper.

Audit committees will want to understand how the company is using AI and verify that it is doing so in a responsible way for the key areas where they have responsibility. Whether partially or fully responsible, it is important that audit committees upskill on AI so they can engage with management, ask good questions and challenge leadership when necessary.

AI and key areas of audit committee oversight

Common questions to ask

As the audit committee engages with various C-suite executives through its oversight role, a few foundational questions will help shape conversations.

- **Strategic opportunities:** How are you using AI in your function? What are the immediate and larger transformative opportunities? What are your competitors doing and how are you staying ahead of them?
- **Responsible AI:** How are you driving the responsible use of AI through strong governance and risk frameworks? How are you testing AI models for accuracy, completeness, reliability, data bias and other risks prior to deployment? How are humans in the loop to validate outcomes? What is the plan for ongoing monitoring?
- **Higher-risk AI models:** Which AI models are you using that you deem higher risk, and why? What data are you using for these models? How are you addressing development, deployment and validation for these models?
- **Talent:** What is the impact of AI on your function's talent strategy? How are you monitoring whether your team is getting upskilled on AI?

Determining AI models that create higher risk

Companies need to determine which AI models they deem to present higher risk to the organization. The models may be those that, if they fail, malfunction or are misused could significantly impact a company's reputation, financial results or create potential legal issues, for example. Management should consider different factors to make the determination, including the training data used, whether sensitive data is involved, whether the model is external-facing and even the volume of activity, along with other factors.

Financial reporting, internal controls and financial statements

One of the audit committee's primary roles is to oversee the integrity of the company's financial statements and related disclosures as well as the processes and controls in place governing the recording, aggregation and reporting of that data and information. As companies begin to evaluate and use AI in the financial reporting process, audit committees will want to understand where, why and how they are using it and verify that appropriate controls and processes are in place to manage unique AI-related risks. It is essential to remember that, despite the advanced capabilities of AI, human oversight remains crucial, and employees are responsible for confirming the accuracy of the outcomes generated by these models.

Strategic opportunities

AI can present finance leaders with significant opportunities to make the finance function more insightful and proactive in driving business performance and creating strategic value. By leveraging AI, finance departments can enhance their forecasting capabilities, streamline reporting processes and generate actionable insights that drive informed decision-making, for example.

As many finance functions are already in the midst of digital transformation, integrating AI should complement these ongoing efforts.

AI in financial reporting: real-world applications*

- **Using AI agents to ingest and validate large volumes of data to automate draft disclosures and support complex accounting estimates:** These intelligent systems are being used to interpret context, automate complex workflows, make recommendations and continuously learn and improve.
- **Analyzing variances and providing commentary:** AI can transform numerical data into text, producing written commentary more quickly to save time and uncover new insights.
- **Benchmarking and writing draft financial disclosures:** AI can quickly digest complex financial data to write financial disclosures — and benchmark those disclosures against peer companies on a continuous basis.
- **Querying financial information for real-time insights:** AI enables companies to leverage a catalog of prior and current reports — across a wider range of sources — to more quickly and fully respond to questions about financial results and public statements or filings.
- **Identifying trends in SEC filings:** AI can extract filing data from EDGAR, summarize trends and perform industry analyses at speed.

* While AI is being used in real-world applications, it is essential for humans to be in the loop for managing, reviewing and overseeing AI systems and their outcomes.

Maintaining trust with Responsible AI

As AI is used in the financial reporting process, audit committees should discuss how AI risks are managed. A particular focus should be on data quality as this area can have a large bearing on the accuracy and reliability of financial reporting and financial statements.

Audit committees should understand how internal control over financial reporting is changing. For example, has the company updated its controls to address the use of AI agents that perform reviews and approvals that were formerly done by humans? What are the controls and how are outcomes monitored? How are humans involved in monitoring outcomes?

It's important to have a discussion with finance leaders on the Responsible AI practices in place, including policies, procedures and company standards related to the development, deployment and use of AI models. Responsible AI practices should be applied not only to the company's AI models but to those of third parties; companies will want to make sure AI models deliver quality, accurate and reliable outcomes. These practices should be aligned to the company's enterprise-wide Responsible AI program.

Audit committees will likely want to dive deeper into AI models used in financial reporting that the company's risk management program has identified as higher risk. This involves overseeing whether management has assessed the effectiveness of controls for developing, deploying, validating and monitoring these models. The quality of financial statements is crucial to global capital markets, and improperly managed high-risk models could have significant effects.

72%

In the S&P 500, 359 companies (72%) mentioned AI-related risks in their 10-Ks in 2023.

Source: Desiré Carroll, "Analyzing S&P 500 Companies' 10-K Disclosures: Climate and AI," *Center for Audit Quality,* February 24, 2025.

Regulators and standard setters

As companies begin to use AI in financial reporting, regulators and standard setters, like the FASB and SEC, will likely need to address AI use in their rules and standards. Companies should align their AI use with these regulations, as staying informed about developments is important.

Transparency in AI usage is also critical. Many companies are already disclosing how AI applications may create risks in the Risk Factors section of their 10-K reports to help maintain stakeholder trust and meet regulatory expectations.

Audit committees can discuss guarding against "AI washing," in which companies exaggerate or falsely represent their AI capabilities. The SEC has warned against such misleading disclosures, emphasizing the need for truthful and clear communication about AI-related risks and management strategies.

Internal audit

Internal audit can be a key mechanism to help understand and assess whether the company's AI governance and related risk management programs are effective. Additionally, audit committees will want to understand how internal audit is using AI to conduct its audits more effectively and efficiently as well as what the outcomes and findings are from their audits across the company on AI model use and risk management.

Strategic opportunities

AI clearly has the potential to revolutionize how auditing is done. Its ability to process vast amounts of data quickly can enable auditors to enhance their audit plans with more dynamic, data-driven approaches, improving the depth and scope of their controls and transaction testing.

However, AI also brings risks, and AI used by internal audit should be governed with the same rigor as AI used across the company. Audit committees will want to understand how internal auditors are developing, deploying, validating and monitoring AI models, and how they are managing their risks, particularly with regard to data integrity and the reliability of AI-generated information. As in other areas, it is crucial for internal auditors to incorporate human judgment in evaluating AI outcomes for fairness, accuracy, reliability and consistency.

With the use of AI in the internal audit function, audit committees should discuss with the chief audit executive (CAE) how internal audit is evolving and how the technology affects the function's talent strategy and skill sets.

Assessing AI use across the company

The internal audit process can serve as a crucial governance tool to assess the development, deployment and use of AI across the company, providing important assurance to the audit committee. Internal audit should familiarize itself with the company's Responsible AI governance framework, which includes the inventory of AI models, risk taxonomy and the determination of higher-risk AI models, to help effectively guide its audit planning. The annual audit plan should concentrate on AI-related risks with a focus on models that have been classified as high risk by the company's risk management program.

Additionally, the audit committee can leverage internal audit capabilities to assess risks associated with AI models embedded in third-party software in addition to those developed internally.

Audit findings can deliver valuable insights to the audit committee, highlighting successes, risks and challenges associated with AI model use. It is important that the audit committee and the CAE engage in discussions regarding these findings.

AI in internal audit: real-world applications*

- **Enhancing audit planning:** AI can help perform planning activities by consuming various inputs, such as the risk assessment and applicable regulatory requirements, and then draft planning memoranda.
- **Using advanced analytics to improve risk assessment and insights:** AI can incorporate quantitative analytics, pattern analysis and complex data insights into audit plans to help expand risk coverage, quickly detect anomalies and perform continuous monitoring.
- **Improving controls testing:** AI can draft testing procedures based on requirements, identify gaps or duplications in controls and summarize issues to more quickly get to action and remediation.
- **Summarizing walkthroughs:** AI can use reviewed transcripts from walkthrough meetings to summarize process narratives, controls, observations and draft test plans and request lists since walkthrough documentation is often time-consuming and detailed.
- **Drafting audit reports:** AI can create initial draft audit reports, including audit background, executive summary, and observations and conclusions.

* While AI is being used in real-world applications, it is essential for humans to be in the loop for managing, reviewing and overseeing AI systems and their outcomes.

External audit

Just as with internal audit processes, AI has the potential to revolutionize the way external auditors do their work. The audit committee should discuss with the external audit partner where they're using AI in performing the audit with a focus on how they are enabling AI models to produce accurate, reliable and consistent outcomes.

The audit committee will want to understand how AI impacts the external audit team's talent strategy, the audit methodology, and how AI models and tools used are tested and validated. The audit committee can discuss with the external audit partner how regulation on AI could impact the external audit.

Assessing AI risks in financial reporting

External audit plans should adjust to address the company's AI-related risks in financial reporting and the underlying processes and controls. Audit committees should understand these changes. Audit committees will want to pay attention to representations added to the management representation letter specifically related to AI, to understand what representations management has made and the process they undertook to support their responses.

Findings from external audits can provide another valuable source of information to the audit committee on the responsible use of AI models in financial reporting.

Importantly, external auditors should align AI use in audits with its regulator. Audit committees will want to keep up to date for any guidance issued by regulators or changes to standards regarding the use of AI in audits.

Compliance, ethics and fraud deterrence

Audit committees typically have responsibility for overseeing the organization's adherence to applicable laws, regulations, internal policies and the like. They often review compliance and ethics programs to assess their effectiveness and help identify potential risks.

The audit committee can meet with the chief compliance officer (or similar executive) to understand where and how the company is using AI to manage its compliance and ethics programs.

If the full board is not addressing AI regulatory risks, the audit committee can understand how relevant AI regulations are evolving and how those might impact the company. They should understand how management is tracking regulations across the global, federal, state and industry levels — and discuss whether management has sufficient resources and expertise to do this effectively.

State lawmakers introduced almost 700 AI-related bills in 2024. One hundred thirteen (113) were signed into law and another 77 advanced through at least one state legislative chamber.

Business Software Alliance. "2025 State AI Wave Building After 700 Bills in 2024." *BSA.org.* Accessed May 13, 2025.

One area for directors to inquire about is whether the company's legal team has reviewed contractual agreements for potential legal liabilities, indemnity rights, data ownership, data protection and privacy, and other provisions brought about by the company's use of AI.

AI in compliance: real-world applications*

- **Writing compliance policies:** AI can create draft compliance policies based on analyzing compliance rules and policy examples.
- **Understanding regulations:** AI can summarize and analyze the vast number of regulatory requirements across various agencies or global expectations, identify alignment and differences in compliance obligations, and identify opportunities for more effective compliance or potential gaps.

* While AI is being used in real-world applications, it is essential for humans to be in the loop for managing, reviewing and overseeing AI systems and their outcomes.

Detecting anomalies: AI can detect certain anomalies in employee behavior or system access logs using machine learning.

- **Flagging potential risks:** AI can use natural language processing to flag potentially risky communication in emails, chats or documents.
- **Analyzing data for evidence:** AI can assist in forensic data analysis and parse through large volumes of unstructured data (emails, chat logs, reports) to find relevant evidence.

Deterring fraud

AI can play a crucial role in deterring fraud by employing advanced techniques such as anomaly detection and behavioral analysis to help identify and flag suspicious activities in real time.

At the same time, AI can be used to perpetrate fraud by creating "deep fakes" or more sophisticated scams. Deep fakes can include fraudulent documentation, voice cloning, video manipulation and other means to deceive individuals and organizations, potentially facilitating identity theft, misleading financial transactions or spreading misinformation.

For the audit committee's areas of oversight, audit committees can ask C-suite executives how their activities address the potential of fraudulent activities using AI.

The US Federal Bureau of Investigation has been warning consumers since 2020 about the risks of AI use in fraud, citing concerns such as synthetic content on fake social media profiles, spear phishing messages, AI-generated images, video, sound and more. Financial officers at companies can be vulnerable to the same kinds of attacks.

Source: Federal Bureau of Investigation. *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud.* Public Service Announcement No. I-120324-PSA. December 3, 2024.

Risk management

Holistic risk management helps companies manage and mitigate risks while achieving their strategic goals. Audit committees are usually responsible for overseeing policies and processes related to an enterprise risk management (ERM) program. Many audit committees also oversee cybersecurity and data privacy.

With these responsibilities in mind, audit committee members should understand how the company is incorporating AI risks into its ERM program — and whether the ERM program is leveraging AI to drive a more proactive approach to risk management.

Strategic opportunities

AI offers considerable potential to enhance risk management processes by simplifying and transforming data gathering and analysis. With AI, an ERM process can begin to include real-time data analysis and predictive analytics, helping to make its view of potential risks far more dynamic and future-facing compared to ERM's traditional orientation toward historical data. This can allow organizations to identify emerging risks earlier and manage vulnerabilities more proactively.

Maintaining trust with Responsible AI

Companies should identify, assess, rank and manage AI risks, just as they likely do with other risks across the organization.

Not every AI model is the same. A company should consider establishing a risk foundation that includes an inventory of AI use across the organization, a common risk taxonomy, and policies, processes and controls to help manage these risks.

Risk management teams can log AI models used in financial reporting, internal audit or compliance into the company's inventory of AI use. They can evaluate these models using the common risk taxonomy to determine whether any of them carry a higher risk to the organization. A higher risk designation may depend on what training data the model uses, whether sensitive data is involved, whether the model is external facing and even the volume of activity.

Audit committees should understand which models within their oversight responsibility are deemed higher risk by the company, and they'll likely want to dive deeper into understanding these models and how the company is managing those risks.

A key aspect of Responsible AI is the integration of human experience with technological capabilities. This "human-in-the-loop" model is especially important when AI plays a role in high-profile judgments and outcomes — as it does with financial reporting.

Sources of AI risk

- **Data risks:** Risks related to the collection, processing, storage, management and use of data during the training and operation of the AI system
  - This includes addressing how data choices and governance practices can affect the risks of bias in AI models.
- **Model risks:** Risks related to the training, development and performance of the AI system itself
  - This includes conceptual soundness, explainability and interpretability of the model, accuracy and reliability of outcomes, and accountability and oversight for model performance over time.
- **System and infrastructure risks:** Risks related to the acquisition, implementation and operation of an AI system in a broader software and technology environment
- **Legal and compliance risks:** Risks of not complying with applicable laws, rules and regulations
  - This includes privacy regulations and sector-specific and function-specific guidance, all within an increasingly fractured global and US regulatory environment.
- **Use risks:** Risks related to intentional or unintentional misuse, manipulation or attack of AI systems
- **Process risks:** Unforeseen or unmitigated risks that arise from integrating AI into existing workflows
- **Third-party risks:** Risks related to vendors supplying AI-driven or AI-augmented tools, platforms and services. These risks include biased or unreliable models, data privacy issues and insufficient transparency.

AI and cyber risks

Audit committees often oversee cyber risks. They should engage with the chief information security officer (CISO) about how AI is affecting data security and privacy as well as which cyber activities can address this new landscape.

Cybercriminals are often quick to exploit AI, utilizing its capabilities without ethical constraints, which can give them a first-mover advantage in harmful activities. Threat actors can leverage AI to generate more convincing phishing emails, deep-fake videos or audio to impersonate company personnel. This enables them to execute sophisticated fraud and deception campaigns on a large scale. Given these threats, it's important to invest in training and awareness programs to help educate employees.

On the other hand, AI's potential to bolster cybersecurity defenses is significant. AI can transform threat intelligence, detecting threats more quickly and accurately by reviewing logs in real time, recommending the appropriate employee access level for sensitive IT systems and allowing for more timely, proactive measures against potential breaches. There are many benefits in using AI to manage cyber risks at a company.

Conclusion

As we look to the future, the integration of AI into business operations is expected to continue to evolve, presenting both unprecedented opportunities and risks. Audit committees can play a pivotal role in overseeing the strategic and responsible use of AI within financial reporting, internal audit, external audit, and compliance and ethics.

How PwC can help

To have a deeper discussion about how this topic might impact your business, please contact your engagement partner or one of the following PwC's contacts:

Ray Garcia
Leader, Governance Insights Center
ray.r.garcia@pwc.com

Stephen G. Parker
Partner, Governance Insights Center
stephen.g.parker@pwc.com

Barbara Berlin
Managing Director, Governance Insights Center
barbara.berlin@pwc.com

Tracey Lee Brown
Director, Governance Insights Center
tracey-lee.y.brown@pwc.com