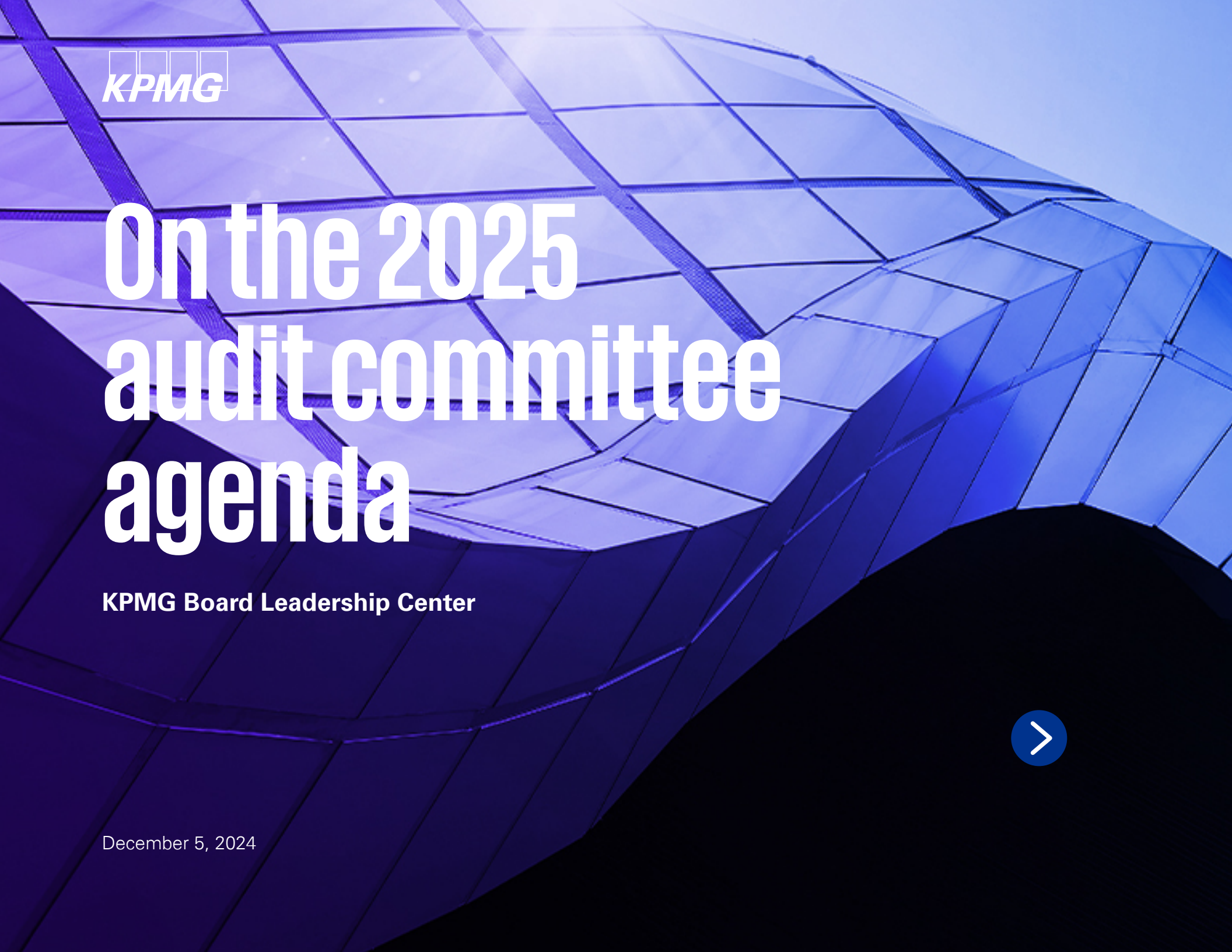


# On the 2025 audit committee agenda

**KPMG Board Leadership Center**

December 5, 2024

Audit committees can expect their company's financial reporting, compliance, risk, and internal control environment to be put to the test in 2025. In addition to existing challenges—from global economic volatility, the wars in Ukraine and the Middle East to cyberattacks, preparations for US and global climate and sustainability reporting requirements, and advances in artificial intelligence (AI)—the change in administration could have a significant impact on the business and risk environment that companies must navigate. Audit committees should take a hard look at their skill sets and agendas. Does the committee have the leadership, composition, and agenda time to carry out its core oversight responsibilities—financial reporting and internal controls—along with the growing range and complexity of other risks?

Drawing on insights from our survey work and interactions with audit committees and business leaders, we highlight nine issues to keep in mind as audit committees consider and carry out their 2025 agendas:

**Stay focused on financial reporting and related internal control risks—job number one.**

**Clarify the role of the audit committee in the oversight of generative AI (GenAI), cybersecurity, and data governance.**

**Understand how technology is affecting the finance organization's talent, efficiency, and value-add.**

**Reinforce audit quality and stay abreast of changes to PCAOB auditing standards.**

**Monitor management's preparations for new climate reporting frameworks/standards.**

**Make sure internal audit is focused on the company's critical risks—beyond financial reporting and compliance—and is a valuable resource for the audit committee.**

**Probe whether management has reassessed the company's compliance and whistle-blower programs in light of the DOJ's September Evaluation of Corporate Programs guidance.**

**Stay apprised of tax legislative developments in Washington and the potential impact on the company and its operations.**

**Take a fresh look at the audit committee's composition and skill sets.**

# Stay focused on financial reporting and related internal control risks—job number one.

Focusing on the financial reporting, accounting, and disclosure obligations posed by the current geopolitical, macroeconomic, and risk landscape will be a top priority and major undertaking for audit committees in 2025. Key areas of focus for companies' 2024 10-K and 2025 filings should include:

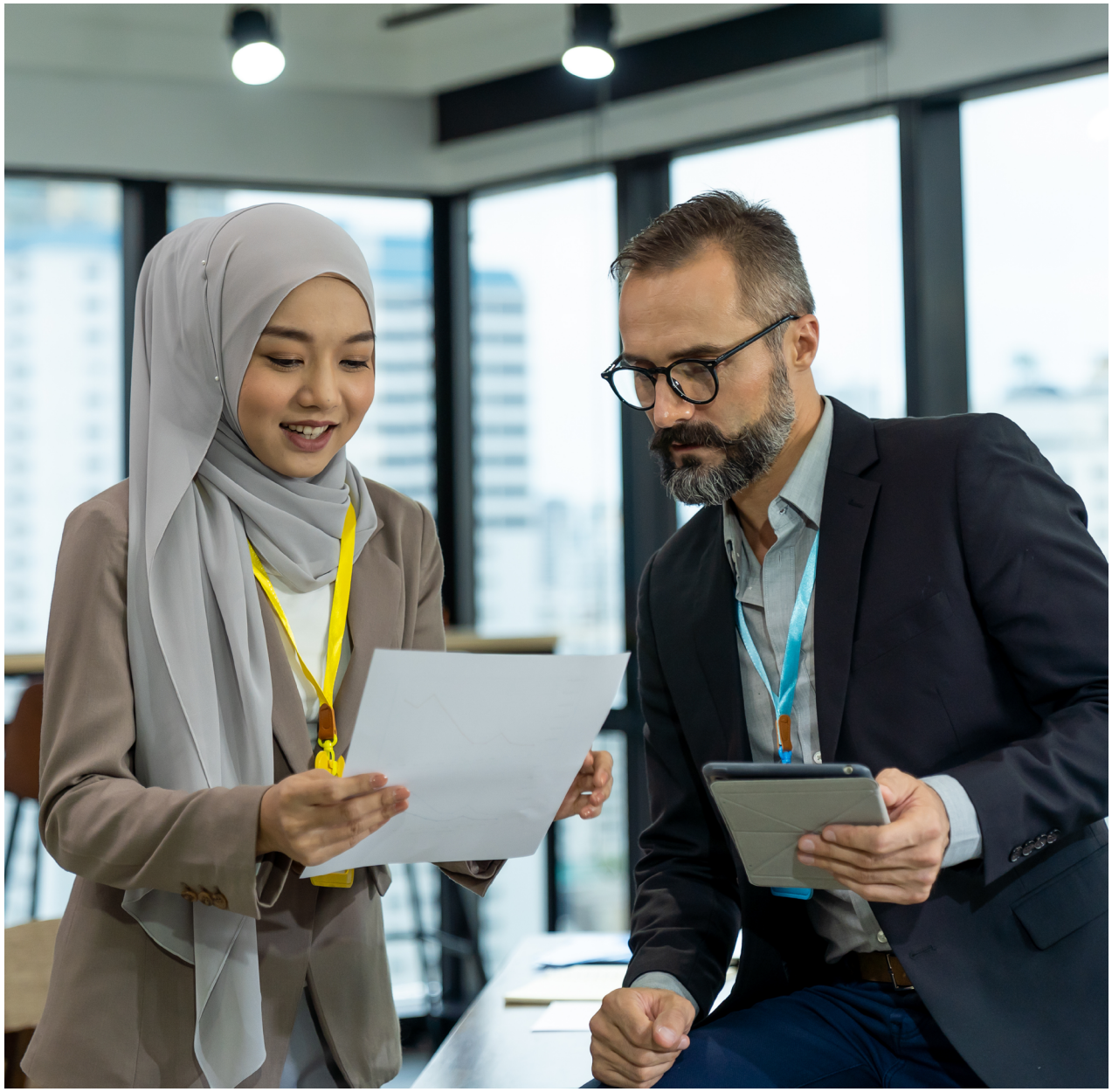
*Forecasting and disclosures.* Among the matters requiring the audit committee's attention are disclosures regarding the impact of the wars in Ukraine and the Middle East; government sanctions; supply chain disruptions; heightened cybersecurity risk, inflation, interest rates, and market volatility; preparation of forward-looking cash-flow estimates; impairment of nonfinancial assets, including goodwill and other intangible assets; impact of events and trends on liquidity; accounting for financial assets (fair value); going concern; and use of non-GAAP metrics. With companies making more tough calls in the current environment, regulators are emphasizing the importance of well-reasoned judgments and transparency, including contemporaneous documentation to demonstrate that the company applied a rigorous process. Given the fluid nature of the long-term environment, disclosure of changes in judgments, estimates, and controls may be required more frequently.

*Internal control over financial reporting (ICOFR) and probing control deficiencies.* Given the current risk environment, as well as changes in the business, such as acquisitions, new lines of business, digital transformations, etc., internal controls will continue to be put to the test. Discuss with management how the current environment and regulatory mandates affect management's disclosure controls and procedures and ICOFR, as well as management's assessment of the effectiveness of ICOFR. When control deficiencies are identified, probe beyond management's explanation for "why it's only a control deficiency" or "why it's not a material weakness" and help provide a balanced evaluation of the deficiency's severity and cause. Is the audit committee—with management—regularly taking a fresh look at the company's control environment? Have controls kept pace with the company's operations, business model, and changing risk profile?

*Nonfinancial disclosures.* In 2025, companies should expect the SEC to continue to prioritize nonfinancial disclosures, particularly disclosures regarding climate, cybersecurity, and AI, including the adequacy of internal controls and disclosure controls and procedures to support the company's disclosures.

Despite the stay of its final climate rules, the SEC continues to issue comment letters on climate disclosures based on the 2010 Commission Guidance Regarding Disclosure Related to Climate Change and its 2021 sample letter. As to cybersecurity disclosures, company procedures for identifying and reporting cyber incidents and risks will be under even greater scrutiny given the new Form 8-K reporting requirements for material cybersecurity incidents as well as the SEC's recent enforcement actions in this area. Regarding AI, in a June 2024 statement, Eric Gerding, director of the SEC's Division of Corporation Finance, highlighted AI as a disclosure priority for the SEC and explained in some detail how the division will assess company disclosures regarding AI-related opportunities and risks. In a February 2024 speech focusing on AI and AI-related risks, Chair Gary Gensler warned about "AI washing" or making inflated claims about the use of AI, which have now been the focus of SEC enforcement actions.

Audit committees should task management with reassessing the adequacy of the company's internal controls and disclosure controls and procedures to support the company's current climate and AI disclosures (including disclosures contained in SEC filings, as well as voluntary disclosures), and reassess the company's processes and procedures for identifying and escalating potentially significant cybersecurity incidents and risks to ensure timely analysis and disclosure of those determined to be material. As disclosures under Item 1.05 of Form 8-K are limited to material cybersecurity incidents, it is essential that companies establish and maintain protocols and processes for making materiality determinations.



# Clarify the role of the audit committee in the oversight of GenAI, cybersecurity, and data governance.

The explosive growth in the use of GenAI has emphasized 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 or, in some cases, developing data governance practices.

As a result, many boards are probing whether the company's data governance framework and interrelated AI, GenAI, and cybersecurity governance frameworks are keeping pace. A key question for boards is how to structure oversight of these areas at the full board and committee levels, including the audit committee. In assessing the audit committee's oversight responsibilities in these areas, we recommend the following areas of focus:

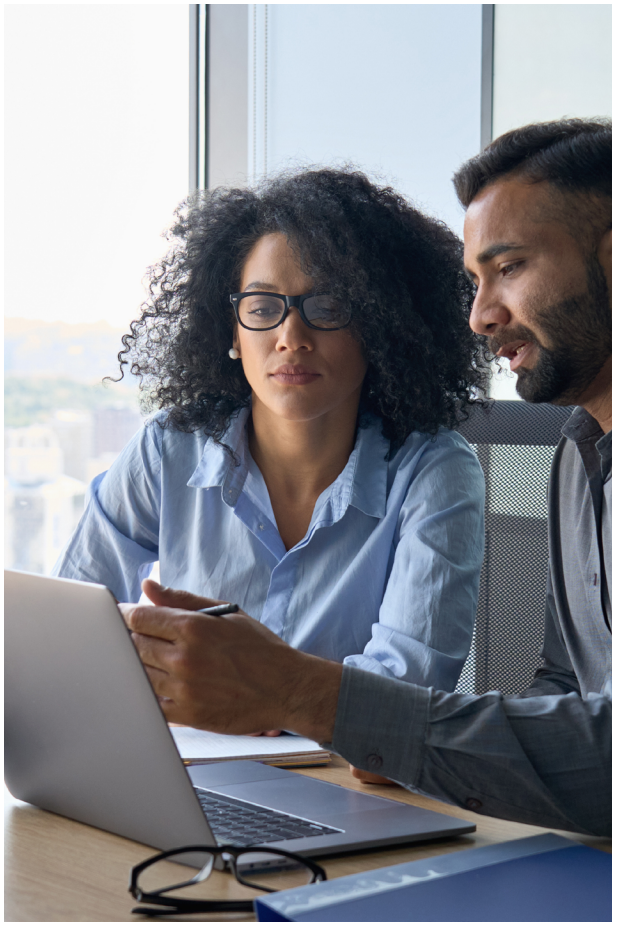
*Assessing audit committee oversight responsibilities for GenAI.* Many boards are still considering how best to oversee AI and GenAI and the appropriate roles of the full board as well as standing committees as they seek to understand GenAI's potential impact on strategy and the business model. As we discuss in **On the 2025 board agenda**, oversight for many companies is often at the full board level—where boards are seeking to understand the company's strategy to develop business value from GenAI and monitor management's governance structure for the deployment and use of the technology. However, many audit committees already may be involved in overseeing specific GenAI issues, and it is important to clarify the scope of the audit committee's responsibilities. GenAI-related issues for which the audit committees may have oversight responsibilities include:

- Oversight of compliance with evolving AI, privacy, and intellectual property laws and regulations globally
- Use of GenAI in the preparation and audit of financial statements and drafts of SEC and other regulatory filings
- Use of GenAI by internal audit and the finance organization, and whether those functions have the necessary talent and skill sets
- Development and maintenance of internal controls and disclosure controls and procedures related to AI and GenAI disclosures, as well as controls around data.

*Assessing audit committee oversight responsibilities for cybersecurity and data governance.* For many companies, much of the board's oversight responsibility for cybersecurity and data governance has resided with the audit committee. With the explosive growth in GenAI and the significant risks posed by the technology, many boards are rigorously assessing their data governance and cybersecurity frameworks and processes.

Given the audit committee's heavy agenda, it may be helpful to have another board committee assume a role in the oversight of data governance and perhaps cybersecurity.

# Understand how technology is affecting the finance organization's talent, efficiency, and value-add.



Finance organizations face a challenging environment—addressing talent shortages, while at the same time managing digital strategies and transformations and developing robust systems and procedures to collect and maintain high-quality climate and sustainability data both to meet investor and other stakeholder demands and in preparation for US, state, and global disclosure requirements. At the same time, many are contending with difficulties in forecasting and planning for an uncertain environment. As audit committees monitor and help guide the finance organization's progress, we suggest two areas of focus:

- GenAI goes a long way toward solving one of the biggest pain points in finance: manual processes. Labor-intensive systems increase the risk of human errors, consume valuable resources, and limit real-time insights. At the same time, given the broad role for finance in strategy and risk management, finance professionals can play a role in spearheading the company's use and deployment of GenAI. GenAI and the acceleration of digital strategies and transformations presents important opportunities for finance to add greater value to the business.
- Finance organizations also play an important role in many of the company's climate and sustainability initiatives. For example, many finance organizations have been assembling or expanding management teams or committees charged with preparing for US, state, and global climate and sustainability disclosure rules—e.g., identifying and recruiting climate and sustainability talent and expertise; developing internal controls and disclosure controls and procedures; and putting in place technology, processes, and systems.

It is essential that the audit committee devote adequate time to understanding finance organization's GenAI and digital transformation strategy and climate/sustainability strategy, and help ensure that finance is attracting, developing, and retaining the leadership, talent, skill sets, and bench strength to execute those strategies alongside its existing responsibilities. Staffing deficiencies in the finance department may pose the risk of an internal control deficiency, including a material weakness.

# Reinforce audit quality and stay abreast of changes to PCAOB auditing standards.

Audit quality is enhanced by a fully engaged audit committee that sets the tone and clear expectations for the external auditor and monitors auditor performance rigorously through frequent, quality communications and a robust performance assessment.

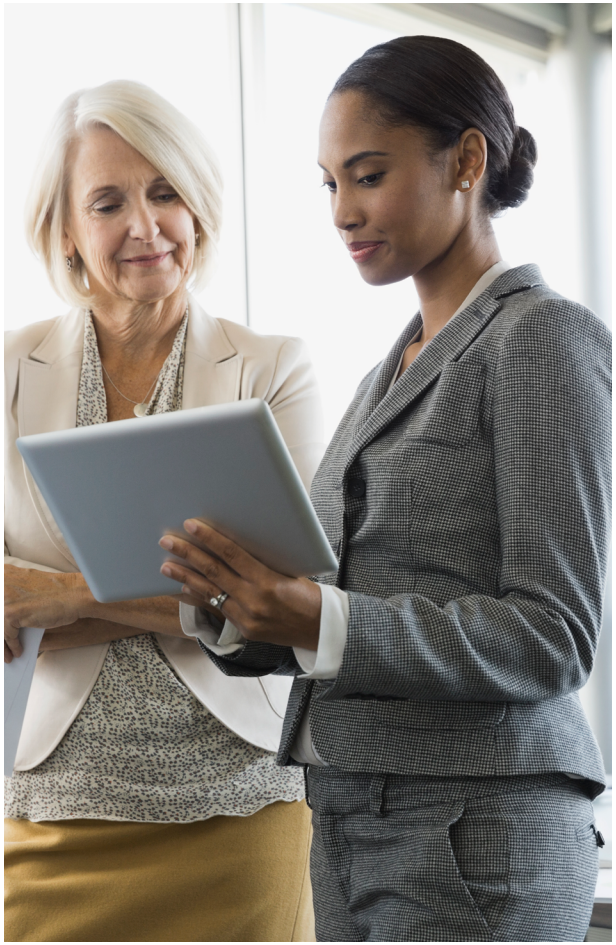
In setting expectations for 2025, audit committees should discuss with the auditor how the company's financial reporting and related internal control risks have changed—and are changing—in light of the geopolitical, macroeconomic, regulatory, and risk landscape, as well as any changes in the business.

Set clear expectations for frequent, open, candid communications between the auditor and the audit committee, beyond what is required. The list of required communications is extensive and includes matters about the auditor's independence as well as matters related to the planning and results of the audit. Taking the conversation beyond what is required can enhance the audit committee's oversight, particularly regarding the company's culture, tone at the top, and the quality of talent in the finance organization.

Audit committees should probe the audit firm on its quality control systems that are intended to drive sustainable, improved audit quality—including the firm's implementation and use of new technologies such as AI. In discussions with the auditor regarding the firm's quality control systems, consider the results of PCAOB inspections, Part I and Part II, and internal inspections and efforts to address deficiencies.

Discussions should also include the status of the firm's preparations for the PCAOB's new quality control standard, QC 1000, *A Firm's System of Quality Control,* which the SEC approved in September 2024. QC 1000 will require audit firms to identify specific risks to audit quality and design a quality control system that includes policies and procedures to mitigate these risks. Audit firms will also be required to conduct annual evaluations of their quality control systems and report the results of their evaluation to the PCAOB on a new Form QC. QC 1000 is effective on December 15, 2025, with the first annual evaluation covering the period beginning on December 15, 2025, and ending on September 30, 2026.

Audit committees should also monitor developments in the PCAOB's proposal on noncompliance with laws and regulations (NOCLAR), which could significantly increase auditors' responsibilities related to NOCLAR. Due to the PCAOB's recent deferral of action on the proposed NOCLAR standard to 2025, there is uncertainty regarding the proposal.



# Monitor management's preparations for new climate reporting frameworks/standards.

Despite the uncertainty associated with the **SEC** and **California** climate mandates, companies may have to comply with multiple inconsistent laws and will need to determine how best to structure their compliance and reporting programs to address new and complex climate disclosure requirements.

Given these near-term demands and growing consensus around common, comparable reporting standards—likely in accordance with the standards of the International Sustainability Standards Board, which incorporate the Task Force on Climate-related Financial Disclosures standards and Greenhouse Gas (GHG) Protocol—audit committees should closely monitor the state of management's preparations for new climate reporting frameworks/standards.

The uncertainty associated with the SEC's climate disclosure rules is unlikely to temper the forces demanding climate disclosures by other means. Whether the SEC rules are upheld, struck down in whole or part, amended, or abandoned, pressure from investors, stakeholders, and other regulators continues to drive the momentum toward detailed climate and sustainability disclosures. Even in the absence of legally required disclosures, many companies will continue to issue voluntary sustainability and climate-related reports. Moreover, many companies will be subject to European Union and other mandatory reporting regimes. Companies not subject to mandatory climate reporting may be asked to provide climate information to companies to which they provide products and services.

Many companies will be impacted by more than one disclosure regime, and in that case, it is important to assess the level of interoperability between the relevant regulations in order to mitigate the impact of having to comply with multiple regulations at or near the same time. Preparation is about more than disclosures; it could require reassessments of the company's climate-related risk management and board oversight processes, and other governance processes that are the subject of the disclosures.

In the coming months, a priority for audit committees will be to monitor the state of management's preparations. A key question is whether management has the necessary talent, resources, and expertise—internal and external—to gather, organize, calculate, assure, and report the necessary climate data, such as GHG emissions, and to develop the necessary internal controls and disclosure controls and procedures to support the regulatory and voluntary climate disclosures. For many companies, this will require a cross-functional management team from legal, finance, sustainability, risk, operations, IT, HR, and internal audit. Identifying and recruiting climate and GHG emissions expertise for a climate team—which may be in short supply—and implementing new systems to automate the data-gathering process will be essential.

As discussed in **Oversight of climate disclosures: SEC stay shouldn't mean stop**, we recommend the following areas for audit committees to focus in addition to management's climate-related expertise and resources:

- Management's plans to meet compliance deadlines
- Considerations of materiality and double materiality
- Disclosure controls and procedures, and internal controls.

Preparations will be a complex and expensive undertaking, involving difficult interpretational issues, and likely may take months or perhaps years for some companies, especially for multinational organizations. The design and build of a functioning sustainability reporting process that meets regulatory needs will be an iterative process that will take time. Due to this, it is important that audit committees keep the topic on their agendas and continue to challenge management on progress towards compliance.

# Make sure internal audit is focused on the company's critical risks—beyond financial reporting and compliance—and is a valuable resource for the audit committee.

At a time when audit committees are wrestling with heavy agendas and issues like GenAI, ESG, supply chain disruptions, cybersecurity, data governance, and global compliance are putting risk management to the test, internal audit should be a valuable resource for the audit committee and a crucial voice on risk and control matters. This means focusing not just on financial reporting and compliance risks, but on critical operational, GenAI and other technology risks and related controls, as well as ESG risks.

ESG-related risks include human capital management—from diversity to talent, leadership, and corporate culture—as well as climate, cybersecurity, data governance and data privacy, and risks associated with ESG disclosures. Disclosure controls and procedures and internal controls should be a key area of internal audit focus. Clarify internal audit's role in connection with ESG risks and enterprise risk management more generally—which is not to manage risk, but to provide added assurance regarding the adequacy of risk management processes. Does the finance organization have the talent it needs? Do management teams have the necessary resources and skill sets to execute new climate and ESG initiatives? Recognize that internal audit is not immune to talent pressures.

Given the evolving geopolitical, macroeconomic, and risk landscape, reassess whether the internal audit plan is risk-based and flexible enough to adjust to changing business and risk conditions. Going forward, the audit committee should work with the chief audit executive and chief risk officer to help identify the risks that pose the greatest threat to the company's reputation, strategy, and operations, and to help ensure that internal audit is focused on these key risks and related controls. These may include industry-specific, mission-critical, and regulatory risks; economic and geopolitical risks; the impact of climate change on the business; cybersecurity and data privacy; risks posed by GenAI and digital technologies; talent management and retention; hybrid work and organizational culture; supply chain and third-party risks; and the adequacy of business continuity and crisis management plans.

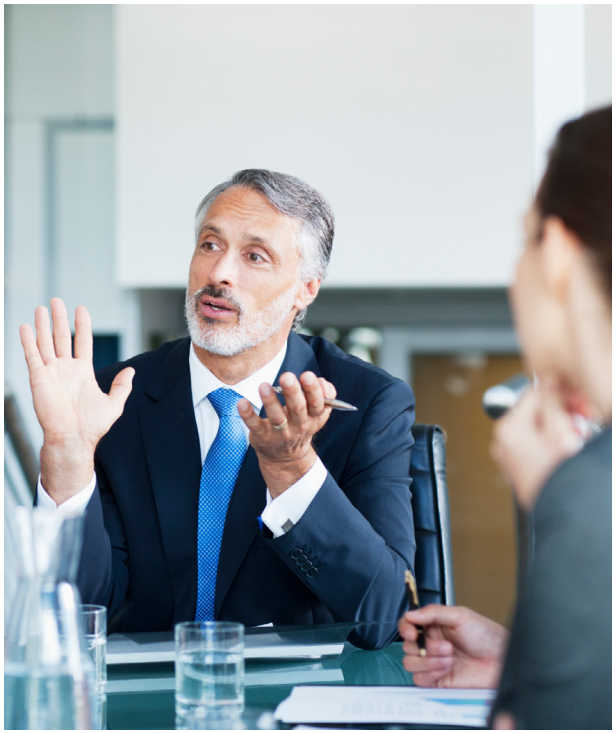
Internal audit's broadening mandate will likely require upskilling the function. Set clear expectations and help ensure that internal audit has the talent, resources, skills, and expertise to succeed—and help the chief audit executive think through the impact of digital technologies on internal audit.

# Probe whether management has reassessed the company's compliance and whistle-blower programs in light of the DOJ's September Evaluation of Corporate Compliance Programs guidance.

In September, the US Department of Justice (DOJ) released a revised version of its guidance for Evaluation of Corporate Compliance Programs (Guidance), which is a tool prosecutors use to evaluate a company's compliance program in determining how to resolve a criminal investigation.[1] The revised Guidance focuses on the risks posed by emerging technologies, such as AI, as well as whistleblower protections, and important lessons learned "from both the company's own prior misconduct and from issues at other companies to update their compliance programs and train employees."

In prepared remarks, Principal Deputy Assistant Attorney General Nicole M. Argentieri stated that the revised Guidance includes an evaluation of how companies are assessing and managing the risks related to the use of new technology such as AI both in their business and in their compliance programs.[2]

> Under the [revised Guidance], prosecutors will consider the technology that a company and its employees use to conduct business, whether the company has conducted a risk assessment of the use of that technology, and whether the company has taken appropriate steps to mitigate any risk associated with the use of that technology. For example, prosecutors will consider whether the company is vulnerable to criminal schemes enabled by new technology, such as false approvals and documentation generated by AI. If so, we will consider whether compliance controls and tools are in place to identify and mitigate those risks, such as tools to confirm the accuracy or reliability of data used by the business. We also want to know whether the company is monitoring and testing its technology to evaluate if it is functioning as intended and consistent with the company's code of conduct.



The revised Guidance also includes questions designed to evaluate whether companies are encouraging employees to speak up and report misconduct, and whether a compliance program has appropriate resources and access to data, including to assess its own effectiveness.

Given the significant risks posed by GenAI and the focus of regulators such as the DOJ and SEC on how companies are managing and mitigating the risks posed by the technology, companies should reassess their compliance and whistleblower programs and update the programs as appropriate.

[1] U.S. Department of Justice Criminal Division Evaluation of Corporate Compliance Programs (updated September 2024).

[2] Principal Deputy Assistant Attorney General Nicole M. Argentieri Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute, September 23, 2024.

# Stay apprised of tax legislative developments in Washington and the potential impact on the company and its operations.

The new administration's policy agenda—from infrastructure investments and business incentives to tax and regulatory priorities—will shape the business environment for years to come. As companies and their boards consider the policy implications, tax policy should be front and center given the potential impacts on cash flow, investment location, and the business landscape generally.

With $4 trillion in tax cuts from the 2017 Tax Cuts and Jobs Act (TCJA) set to expire at the end of next year, 2025 is going to be a big year for tax as House and Senate Republicans are expected to negotiate extending some of its provisions. The White House will require Congress to take the lead on legislating a solution to the 2025 tax cliff, and philosophical shifts in both parties since the TCJA was enacted make what either might do less predictable.

Ultimately, the tax picture that emerges will be driven by a combination of budgetary, fiscal, and political realities, which makes it difficult to predict. Boards and audit committees should prompt deeper conversations with management about how their companies are preparing for a range of possibilities, including by asking management about the type of scenario planning being done; understanding the variables that may be more "forecastable" and looking at the impacts on cash flow; and considering how best to monitor state, federal, and global regulatory developments.

These and other considerations can help the audit committee support management in thinking through various scenarios and positioning the company as the post-election policy landscape unfolds.

# Take a fresh look at the audit committee's composition and skill sets.

The continued expansion of the audit committee's oversight responsibilities beyond its core oversight responsibilities (financial reporting and related internal controls, and internal and external auditors) has heightened concerns about the committee's bandwidth and composition and skill sets. Assess whether the committee has the time and the right composition and skill sets to oversee the major risks on its plate. Such an assessment is sometimes done in connection with an overall reassessment of issues assigned to each board standing committee.

In making that assessment, we recommend three areas to probe as part of the audit committee's annual self-evaluation:

- Does the committee have the bandwidth and members with the experience and skill sets necessary to oversee areas of risk beyond its core responsibilities that it has been assigned? For example, do some risks, such as mission-critical risks as well as supply chain issues and geopolitical risk, require more attention at the full board level—or perhaps the focus of a separate board committee?
- How many committee members have deep expertise in financial accounting, reporting, and control issues? Is the committee relying only on one or two members to do the "heavy lifting" in the oversight of financial reporting and controls?
- As the committee's workload expands to include oversight of disclosures of nonfinancial information—including cybersecurity, climate, GenAI, and other environmental and social issues—as well as related disclosure controls and procedures and internal controls, does it have the necessary financial reporting and internal control expertise to effectively carry out these responsibilities as well as its core oversight responsibilities? Does the committee need the input from experts in order to discharge its oversight duties?

With investors and regulators focusing on audit committee composition and skill sets, this is an important issue for audit committees.

## About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas—from strategy, risk, talent, and sustainability to data governance, artificial intelligence, audit quality, proxy trends, and more. Learn more at **kpmg.com/blc**.

## Contact us

**kpmg.com/us/blc**
**T:** 800-808-5764
**E:** **us-kpmgmktblc@kpmg.com**

**Learn about us:** **kpmg.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.