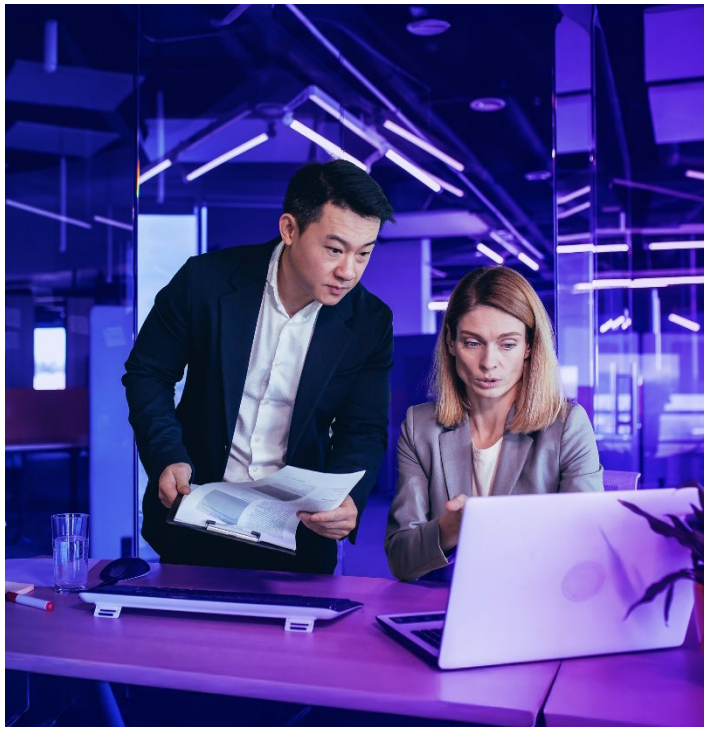
KPMG

On the 2026 audit committee agenda

KPMG RAAD Board Program

On the 2026 audit committee agenda

As the pace of change and complexity in the business environment continues to pressure management and put companies on less-solid footing, the focus and effectiveness of the audit committee will be paramount to investor confidence.



Drawing on insights from our survey work and interactions with audit committees and business leaders, we highlight seven issues to keep in mind as audit committees consider and carry out their 2026 agendas:

Financial reporting
Continue to focus on the effects of volatility –tariff-related, economic, and geopolitical– on financial reporting and related internal control risks

Governance
Clarify the role of the audit committee in the oversight of AI, cybersecurity, and data governance

Finance organization
Understand how technology is affecting talent, efficiency, and value-add

Sustainability
Monitor management's preparations for (updated) sustainability reporting frameworks and standards

Audit quality
Reinforce audit quality and set clear expectations for frequent, candid, and open communication with the external auditor

Internal audit
Help maintain internal audit's focus on the company's critical risks, beyond financial reporting and compliance

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

Financial reporting

Continue to focus on the effects of volatility: tariff-related, economic, and geopolitical

Key areas of focus for companies' 2025 annual reports

Continuing tariff uncertainty

Oversight of the financial reporting, accounting, and disclosure requirements posed by tariff uncertainty will remain a top priority for audit committees in 2026. Key areas of financial reporting that can be most susceptible to the effects or potential effects of tariffs include revenue recognition, inventory costs and associated impairment risk, credit losses, going concern, and others. Actual impacts largely depend on the industry and geographies the company operates in.

Forecasting and disclosures

Other matters requiring the audit committee's attention include disclosures regarding the impact of global conflicts, sanctions, export controls, supply chain disruptions, heightened cybersecurity risk, inflation, interest rates, and market uncertainties. Transparent, well-documented judgments, particularly those which are forward looking and used within forecasts, will be essential as regulators emphasise rigorous processes and timely updates to estimates and controls. Given the fluid nature of the long-term environment, disclosure of changes in judgments, estimates, and controls may be required more frequently.

Transparent disclosures in annual reports are essential for communicating the impact of ongoing volatility on a company's financial position, internal controls, and risk profile. High-quality disclosures enable stakeholders to understand management's judgments and the company's response to emerging risks, supporting informed decision-making in a rapidly evolving environment.

Regulator priorities over 2025 annual reports

To promote the consistent application of financial and sustainability reporting requirements, both the European securities regulator, ESMA, and the Dutch regulator, AFM, have issued its priorities for 2025 annual reports, which include:

- IFRS financial statements: (i) Geopolitical risks and uncertainties and (ii) Segment reporting
- Sustainability statements: (i) Materiality considerations in reporting under the European Sustainability Reporting Standards (ESRS) and (ii) Scope and structure of the sustainability statements
- ESEF digital reporting: Common ESEF filing errors found in the Statement of Cash Flows

In addition, the regulators have highlighted the importance of connectivity between financial and sustainability information, recent IFRS developments, and consistent use of alternative performance measures. Furthermore, the AFM has specifically to the Dutch context, additionally highlighted the updated Corporate Governance Code 2025.

AI, and cybersecurity disclosures

Audit committees should consider tasking management with assessing the adequacy of the company's internal controls to support the company's disclosures about the company's use of AI, the associated risks, and the company's governance of the technology. Management should also reassess the company's processes and procedures for identifying and escalating potentially significant cybersecurity incidents and risks to ensure a timely and an effective response and disclosure of those determined to be material.

Governance

Clarify the role of the audit committee in the oversight of AI, cybersecurity and data

As companies continue to move forward with investment in and deployment of AI in all its forms, a key question for boards is how to structure oversight of AI at the full board and committee levels, including the audit committee. For many companies, oversight is often at the full board level—where boards are seeking to understand the company's strategy for developing business value from AI and its potential impacts on the business model and workforce, while monitoring management's governance structure for the deployment and use of the technology.

However, many audit committees already may be involved in overseeing specific AI-related issues, and it is important to clarify the scope of the audit committee's responsibilities. AI-related issues for which the audit committees may have oversight responsibilities include:

- AI and data governance, including compliance with evolving and diverging AI, Privacy&Data protection, data (non personal data), consumer protection, cybersecurity, and intellectual property laws and regulations, including those which are driven by the EU.
- Examples of these latter are the EU's AI Act, Data Act, Data Governance Act (DGA), General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) 2 directive.
- Use of GenAI and AI agents in the preparation and audit of financial statements and drafts of (financial and regulatory) filings.
- Use of GenAI and AI agents 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, 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 AI agents as well as increased need for AI and data regulatory compliance, many boards are reassessing their data governance and cybersecurity frameworks and processes to help ensure that they address any increased risks related to the technology. In the process, many boards are reassessing which board committee has the time, expertise, and skill sets to assume a role in the oversight of data governance and perhaps cybersecurity.

New developments regarding EU Digital Omnibus

A new EU development that should also be on the Audit Committee's radar is the impact of the Digital Omnibus, published on 19 November 2025, The EU Digital Omnibus is a legislative package that consolidates and updates existing digital regulations (such as GDPR, the AI Act, and cybersecurity rules) into a single framework. Its purpose is to simplify compliance, reduce overlapping obligations, and modernize the EU's digital rulebook. Amongst others it:

- updates and expands core digital EU law, including the introduction of a single EU platform for incident reporting, e.g. Cybersecurity breaches, data protection violations, and ICT-related incidents
- updates EU AI legislation: including simplifying some measures related to the datasets used to train, validate and verify high-risk AI systems, as well as measures boosting sandboxes in AI, simplifying processes around them.
- introduction of the European Business Wallet, a unified digital identity to business

The EU Digital Omnibus is currently under legislative consideration with final approval expected by mid-to-late 2027.

Finance organization

Understand how technology is affecting talent, efficiency, and value-add

Finance organizations operate in a complex environment, managing talent shortages alongside implementing digital strategies and transformations. They are also tasked with developing systems and procedures that go beyond conventional financial stewardship and reporting, aiming to enhance value by serving as strategic partners within their organizations. At the same time, many are contending with difficulties in forecasting and planning for a volatile environment. As audit committees monitor and help guide the finance organization's progress, we suggest three areas of focus:

- GenAI and AI agents go 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. AI can boost efficiency, but involving humans at vital points in AI workflows is necessary to ensure accuracy, validate results, fix mistakes, add context and provide for judgment.
- Given the broad role of finance in strategy and risk management, finance professionals can play a role in spearheading the company's use and deployment of GenAI and AI agents. These technologies and the acceleration of digital strategies and transformations present important opportunities for finance to add greater value to the business by providing forward-looking insights and analysis in key strategic and risk areas.
- To add value, the finance organization requires talent and expertise beyond traditional finance skills, including talent and expertise in information technology, AI, data analytics, risk management, and strategy, as well as climate and sustainability.

It is essential that the audit committee work closely with the CFO and devote adequate time to understanding the finance organization's AI and digital transformation strategy, where finance can add strategic value to the business, and help ensure that finance is attracting, developing, and retaining the leadership, talent, and skill sets 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.

Sustainability

Monitor management's preparations for (updated) sustainability reporting frameworks and standards

The regulatory uncertainty that defined 2025 is giving way to a clearer path forward in 2026, as greater clarity continues to emerge with multiple climate and sustainability reporting proposals taking shape.

EU developments

In February 2025, the European Commission released an Omnibus package of proposals to reduce sustainability reporting and due diligence requirements. This includes proposed amendments to the Corporate Sustainability Reporting Directive (CSRD) and Corporate Sustainability Due Diligence Directive aimed at simplifying and streamlining the regulatory framework introduced by both directives while still achieving the overall ambition of the European Green Deal. The proposals include significant changes to CSRD scoping, which could result in only some 5 percent of the companies originally in scope remaining in scope. The proposals are currently being finalized, with a final text expected to become EU law in early 2026. Although uncertainty still abounds, significant changes to the CSRD scoping thresholds are highly likely. As part of the Omnibus package of proposals, another effort is being undertaken to streamline the European Sustainability Reporting Standards (ESRS) and to substantially reduce the volume of disclosures. The simplified version of ESRS is likely to enter into force in late 2026.

US developments

Even without the SEC's climate rule, the significance of current disclosure requirements and their applicability to climate-related matters is not diminished. Audit committees should consider tasking management with refreshing their understanding of the SEC's 2010 disclosure guidance and how it currently applies to their organization.

In California, the California Air Resources Board (CARB) is developing regulations that will underpin the California climate laws, SB-253 (GHG emissions) and SB-261 (climate risks). In October, CARB announced that it is delaying initial rulemaking to the first quarter of 2026. Though CARB announced a delay, it did not change the reporting deadlines in the laws. However, in November, the US Court of Appeals for the Ninth Circuit issued an injunction halting enforcement of SB-261 while an appeal is pending, but SB-253 remains unaffected.

CARB will not enforce SB-261 following the injunction. Once the appeal is resolved, CARB will provide further information and set an alternate date for reporting, as appropriate. Companies can still voluntarily submit their Climate-Related Financial Risk Report.

ISSB developments

The International Sustainability Standards Board (ISSB) has proposed significant amendments to the SASB Standards as part of supporting the high-quality implementation of IFRS Sustainability Disclosure Standards.

IFRS® Sustainability Disclosure Standards are mandatory only in jurisdictions that choose to adopt them. Although the effective date in the IFRS Sustainability Disclosure Standards is January 1, 2024, individual jurisdictions are deciding whether and when companies would be required to apply the standards, akin to the process for adopting IFRS Accounting Standards. Unlike IFRS Accounting Standards, which have become the de facto global language of financial reporting, adoption of IFRS Sustainability Disclosure Standards is varying widely across jurisdictions. This leads to differences in how the standards are adopted, who is required to comply, which requirements apply, and when they become mandatory.

Even in the absence of regulatory-driven required disclosures, many companies will continue to issue voluntary sustainability and climate-related reports, and many may be asked to provide climate information to companies to which they provide products and services.

In 2026, audit committees should help ensure management is not simply tracking regulatory developments but is navigating the intersection of three key challenges: the uncertain timeline in California, the scoping uncertainty in the EU, and the global fragmentation of ISSB adoption. Engagement with management should focus on ensuring companies at least consider a flexible, risk-based reporting strategy that satisfies immediate compliance needs without losing sight of broader market expectations and future regulatory horizons.

Audit quality

Reinforce audit quality and set clear expectations for frequent, candid, and open communication with the external auditor

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 communication and a robust performance assessment.

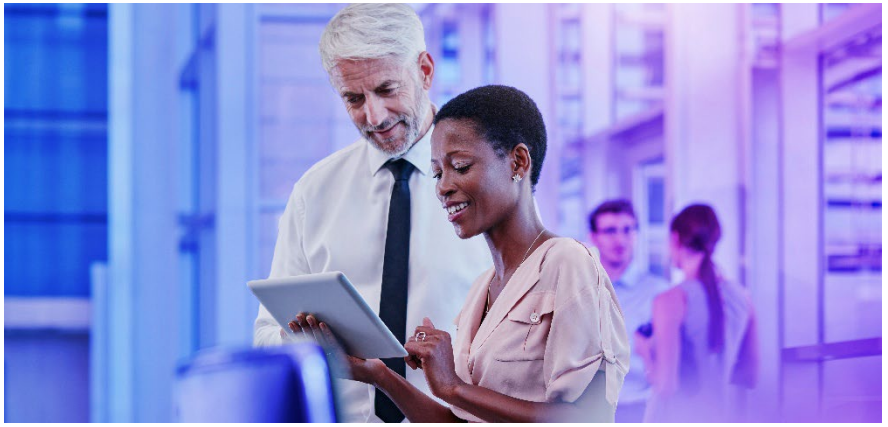
In setting expectations for 2026, audit committees should be sure that their discussions with the auditor include two critical areas: how the company's financial reporting and related internal control risks have changed (and are changing) in light of the unprecedented disruption, volatility, and risks the company will continue to face, as well as changes in the business; and how the company is using AI technologies, including GenAI and AI agents in its financial reporting and related internal control processes.

Set clear expectations for frequent, open, candid communication between the auditor and the audit committee, beyond what's 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's 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.

Given the rapid advancements in the use and deployment of AI, audit committees should discuss with the external auditor how the audit plan provides for assessing risks posed by the company's use of GenAI and AI agents in the financial reporting and related internal control processes. Audit committees should also discuss with the external auditor how the auditor is using GenAI and AI agents in the audit process, how the firm is ensuring audit quality when AI is used, and the impact of the use of AI on audit strategy and resource and talent requirements.

Audit committees should continue to probe the audit firm regarding 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 to drive audit quality. In discussions with the external auditor regarding the firm's internal 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. 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, 2026, with the first annual evaluation covering the period beginning on December 15, 2026, and ending on September 30, 2027.



Internal audit

Help maintain internal audit's focus on the company's critical risks, beyond financial reporting and compliance

Internal audit should be a valuable resource for the audit committee and a crucial voice on risk and control matters. This means not only focusing on financial reporting and compliance risks, but also on critical strategic, operational, AI and other technology risks and related controls, as well as sustainability risks.

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. The audit committee should work with the chief audit executive and chief risk officer to help identify the risks, including industry-specific and mission-critical risks, that pose the greatest threat to the company's reputation, strategy, and operations, and help ensure that internal audit is focused on these key risks and related controls.

The risks posed by the company's use of GenAI and AI agents –and whether the company's governance structure and risk management processes around AI are effective– will likely be an important area of internal audit focus in the coming year. Audit committees will also want to understand how internal audit is using GenAI and AI agents to improve its effectiveness and efficiency. What internal audit workflows can AI agents handle, and what internal audit workflows are AI agents actually handling today? Is internal audit maintaining a human-on-the-loop at critical stages of AI agent workflows?

Internal audit's broadening mandate will likely require upskilling the function to develop and maintain proficiency in areas such as advanced data analytics, AI, cybersecurity risk assessment, climate and sustainability, and operational resilience. 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 GenAI, AI agents, and digital technologies on internal audit.

Audit committee composition

Take a fresh look at the 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, 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 standing board 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? For example, do some risks –e.g., mission-critical risks such as product safety, as well as AI, data governance, cybersecurity, legal/regulatory compliance, culture, supply chain, and geopolitical risk– require more attention at the full board level, or perhaps the focus of another standing 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 a range of risk disclosures –including AI, cybersecurity, and sustainability 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?

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

Contact

Petra Groenland

Co-chair KPMG RAAD Board Program
E. groenland.petra@kpmg.nl
T. 020 6 568 679

Tom van der Heijden

Co-chair KPMG RAAD Board Program
E. vanderheijden.tom@kpmg.nl
T. 020 6 567 520