

Your Q1 audit committee guide

Everything you need to walk into your next audit committee meeting with confidence

April 2026



Table of contents

Topic 01	Oversight of financial reporting in an AI-enabled finance function	03
Topic 02	Monitoring the effects of continued tariff uncertainty	07
Topic 03	Audit committee efficiency and effectiveness remain a top area of focus	10
Topic 04	Connecting with the external auditor post-audit	14
Topic 05	Understanding the SEC's potential shift to semi-annual reporting	17
Topic 06	Current considerations for internal audit oversight	20
Topic 07	What the deals outlook could mean for audit committees	23
Topic 08	Oversight of fraud risk	26
Topic 09	What a reconstituted PCAOB means for audit committees (and auditors)	29
Topic 10	Recurring items for the audit committee agenda	32

Oversight of financial reporting in an AI-enabled finance function

What the audit committee needs to know

AI is moving quickly from experimentation to practical use inside the finance function. Audit committee members may not currently think of the finance function as AI-enabled, but AI capabilities may already be embedded in existing ERP, consolidation, close, and reporting platforms. As a result, AI may be influencing financial reporting even when it is not labeled as an 'AI initiative.'

PwC Pulse Survey findings indicate that roughly one-third of finance leaders report that AI is already in use across many areas of finance, with adoption expected to expand; specific use cases such as forecasting and process automation show meaningful current usage.





AI can be ‘invisible’

“AI may be embedded in existing tools, introduced by vendors, or used informally by employees (‘shadow AI’). Each creates different ICFR and disclosure control implications—and not all will be captured in traditional process documentation unless it is mapped out.”

Where AI is showing up now (and is expected next)

- Close and consolidation analytics (e.g. variance explanations, trend/outlier detection, reconciliation support)
- Drafting and summarizing accounting memos, disclosure language, and management reporting
- Controls support, such as workflow routing, evidence gathering, exception identification, and continuous monitoring
- Estimates and judgments support (e.g. scenario analysis, sensitivity modeling, indicator screening, tax analytics)

AI doesn’t change the fundamentals of financial reporting—but it can change how work is performed, reviewed, and evidenced. The most common risk patterns include:

- Output reliability risk that shows up as plausible but incomplete, inconsistent, or inaccurate outputs
- Data lineage risk—potential for error or noncompliance due to not knowing how data was sourced, transformed, or moved—(e.g. a CRM system showing different data than a dashboard report)
- Access and segregation of duties risk resulting in new tools bypassing established approvals/workflows
- Change management risk evidenced by model/prompt/configuration changes without testing and sign-off
- Evidence and explainability risk (the inability to explain how a result was reached) resulting in a scenario that hinders accountability and compliance

Why is it relevant to the audit committee?

The audit committee oversees the integrity of financial reporting and the effectiveness of internal control over financial reporting (ICFR). AI can shift the company's control environment in ways that are easy to underestimate because adoption may be incremental, decentralized, and fast-paced. The audit committee should devote adequate time to understanding the finance organization's AI and digital transformation strategy. Now is a good time for the audit committee to support strengthened governance and controls in areas under its oversight. Actions should include:

- Reviewing the company's inventory (production and pilots) of AI in finance and confirming there is clear ownership
- Determining what is 'in scope' for ICFR by understanding AI use cases that influence journal entries, estimates, reconciliations, management review controls, key metrics, or disclosures
- Confirming updates to process narratives, risk assessments, and control descriptions for affected processes and controls
- Confirming that controls address validation, review procedures, audit trail, evidence retention, access, and change management
- Supporting internal audit coverage and timing as well as confirming how AI changes the external auditor's risk assessment and evidence expectations in advance of interim testing.

What questions should the audit committee ask?

- Where is management using AI today in the close, consolidation, reporting, or disclosure drafting processes? What activities are expected to move into production in the next 6–12 months?
- Which AI-enabled activities directly influence journal entries, estimates, reconciliations, key metrics, or disclosures, and who is accountable for the final judgment and approval?
- What is management’s process for updating ICFR documentation to reflect AI-enabled activities?
- How does management confirm accuracy, completeness, and consistency of AI-supported analysis or drafts before they influence reporting?
- What is management’s process for preventing or detecting ‘shadow AI’ use in reporting and other critical work processes?
- How has internal audit incorporated AI-related risks into the audit plan for finance processes and ICFR?
- What is internal audit’s process for identifying and assessing unapproved AI use that could affect reporting?
- How does AI use in the financial reporting process affect the external auditor’s risk assessment, reliance on controls this year, and interim testing approach?
- Where has the external auditor seen issues arise when companies introduce AI into finance workflows?



Where to go for more information:

[Oversight in the AI era: understanding the audit committee’s role](#)

[Overseeing the external auditors](#)

[Responsible AI in finance: 3 key actions to take now](#)

[AI agents are here—and they’re transforming finance and reporting](#)

[Responsible AI: Now that AI is part of your business, what does it mean for audits?](#)

Monitoring the effects of continued tariff uncertainty

What the audit committee needs to know

The US Supreme Court's February 20, 2026 decision striking down tariffs imposed under the International Emergency Economic Powers Act (IEEPA) puts tariff uncertainty back into the spotlight. In a 6–3 ruling, the Court held that IEEPA does not provide statutory authority for the President to impose tariffs. The decision effectively eliminates IEEPA as a standalone tariff authority, significantly altering the legal foundation for existing IEEPA-based tariffs. The Court did not provide extensive guidance on the retroactive consequences of its ruling, leaving potential uncertainty regarding refund claims to the lower courts to resolve.

Since the Court did not explicitly rule on the right to a refund of the previously incurred IEEPA tariffs, a company that incurred those tariffs would need to assess, under the relevant legal framework, whether it has a valid legal refund claim against the government. That judgment should be made in the period of the Supreme Court's ruling and re-assessed at each reporting period based on any new information. Importantly, the Supreme Court's ruling is limited to the IEEPA tariffs and does not affect any of the other tariffs that continue to remain in force.

In response to the ruling, President Trump posted online that he had signed an order to impose a 10% global tariff under Section 122 of the Trade Act of 1974 (subsequently raised to 15%), which allows the President to impose tariffs up to 15% for 150 days on nations that have persistent trade imbalances with the US. After that time, the tariffs would require a vote of Congress to be extended. Additionally, other tariffs that the President has already imposed, like the sector-specific tariffs on steel, aluminum, cars, trucks, lumber, and other industries, are imposed under Section 232 of the Trade Expansion Act of 1962 and are outside the scope of the Supreme Court case.

Why is it relevant to the audit committee?

From a financial reporting standpoint, tariff impacts cut across areas directly within the audit committee's oversight responsibility. The financial statement implications related to tariffs may be complex. Beyond cost of sales impacts, management may need to evaluate how refund claims, pricing actions, supply chain reconfiguration, and related judgments flow through inventory accounting, impairment indicators, revenue contracts, income taxes, contingencies, and disclosures. Tariff uncertainty can also affect management's forecasts and earnings guidance by changing assumptions related to costs, pricing, demand, and supply chain execution.

In the post-decision environment, the audit committee can add value by focusing on three practical oversight objectives:

See that the financial reporting implications are being evaluated consistently and early

If management intends to pursue refunds, the audit committee should understand the company's approach to recognition, measurement, classification, and disclosure of potential recoveries, including what documentation supports the amounts and what judgments are being applied.

Maintain discipline in oversight of controls during the volatility

Whether tariffs unwind, persist under different authorities, or shift across products/countries, the underlying processes are often manual or heavily dependent on upstream data. The audit committee should confirm that management and internal audit are identifying where controls may be most vulnerable (e.g. vendor pricing updates, standard cost changes, classification decisions, disclosures).

Coordinate early with the external auditor

Given the complexity and judgment involved, especially about refunds, contingencies, and disclosures, the audit committee should encourage early alignment on external auditor evidence expectations and where specialists may be needed.

What questions should the audit committee ask?

- How has the Supreme Court's February 20 decision changed the company's tariff exposure profile, and what scenarios is management planning for next?
- What is management's process for evaluating the accounting for potential refunds (timing, recognition threshold, measurement, presentation, and disclosure), and what are the key judgments?
- What is management's process for determining where the company is most exposed to tariff uncertainty going forward (e.g. products, geographies, suppliers)?
- How is management scenario-planning outcomes and responses?
- What is management's process for determining which assumptions in forecasts and key estimates are most sensitive to tariff outcomes (e.g. inventory valuation, impairment indicators, revenue pricing/volume, tax assumptions)?
- How has internal audit determined the processes that are at highest risk of control breakdown or inconsistency because of tariff-driven volatility (e.g. procurement, customs data)?
- How is internal audit identifying early-warning indicators, such as manual overrides, reconciliation breaks, and exceptions in approvals, to monitor?
- How does the post-decision environment affect the external auditor's risk assessment?
- What documentation and audit evidence does the external auditor expect to support management's judgments related to refunds, tariff-driven pricing changes, and disclosures?



Where to go for more information:

[US Supreme Court decision on IEEPA tariffs reshapes trade authority and introduces potential refund opportunity](#)

[US Supreme Court invalidates IEEPA tariffs](#)

[Tariffs: the price tag of global trade on financial reporting](#)

[Accounting implications of tariffs](#)

[Disclosure committee essentials](#)

Audit committee efficiency and effectiveness remain a top area of focus



Effectiveness is not about speed—it's about focus

“The objective is to safeguard and expand time for the highest-impact oversight activities such as judgment areas, controls, emerging risks, and audit quality, while reducing time spent on routine activities.”

—**Stephen G. Parker**,
Partner, Governance
Insights Center, PwC

What the audit committee needs to know

Audit committees continue to operate in an environment of expanding oversight while the business and reporting landscape gets more complex. Traditional core responsibilities, such as financial reporting quality, ICFR, and oversight of internal and external audit remain foundational, but the audit committee is increasingly expected to oversee a wider risk landscape. Risks that can affect financial reporting outcomes and stakeholder trust, including cybersecurity and data risk, AI adoption, third-party exposures, evolving regulation, and business model changes are among those being taken on. Our conversations with audit committee members and feedback from peer exchanges frequently center on solutions to help the audit committee maintain efficiency and effectiveness as it deals with a widening scope of its remit and an expanding risk landscape.

Technology is a major accelerant in this evolution. It is changing how companies operate (and therefore how risks manifest), and it is also changing how information is produced and shared with the audit committee. For many audit committees, the issue is no longer a lack of information but about receiving the right information at the right level, early enough to influence outcomes. Streamlining reporting—through clearer executive summaries and dashboards—can help committees focus on issues, trends, and themes, rather than wading through volumes of material. But committee effectiveness is not just about better reporting and agenda content; it's about creating space for the audit committee to spend time where it can add the most value.

Why is it relevant to the audit committee?

Audit committee efficiency and effectiveness are governance imperatives. They affect the audit committee's ability to: (1) oversee the integrity of financial reporting; (2) maintain confidence in ICFR and disclosure controls; and (3) respond quickly when new risks emerge. And because audit committee agendas rarely get shorter, members find that improving effectiveness requires being more intentional about what gets time in meetings and how materials are prepared.

Through our direct interactions with audit committees and via peer exchanges, we highlight a few practical tools and techniques audit committee members are using to create capacity—without compromising oversight:

Start with the annual calendar and 'time budget'

Revisit the annual cycle to confirm that priority responsibilities have adequate time—and that recurring 'housekeeping' topics are handled efficiently. Reviewing the annual calendar should be intentional and include adjustments to prioritize the time allocated to key matters; it should not be 'the same as last year.'

Move from 'updates' to 'issues-based reporting'

Ask management, internal audit, and the external auditor to lead with what changed, what matters, and what decisions or attention are needed from the audit committee—supported by concise dashboards and relevant metrics. This can also reduce repetitive deep dives by focusing discussions on the key items that drive risk.

Use pre-meeting touchpoints to elevate the meeting conversation

Short, targeted pre-meeting briefs (e.g. committee chair with CFO/controller; chair with CAE; chair with engagement partner) can help surface issues early, clarify what the meeting needs to address, and reduce 're-reading the deck' in session.

Make executive sessions more purposeful—before and after meetings

Executive sessions (which include committee members only) are often most valuable when they have a clear objective: before the meeting to surface concerns that might affect the agenda and after to confirm what was learned, what is unresolved, and what follow-up is required. The importance of candid, continuous communication cannot be overstated.

Leverage internal audit more strategically

Internal audit can help the audit committee connect dots across the enterprise, especially where change is putting pressure on controls (systems, reorganizations, third parties, automation). Using internal audit to better understand and oversee the company's evolving risk profile is imperative.

Use technology to improve preparation and follow-through

Secure portals, standardized templates, and clear action tracking improve discipline and reduce cycle time. Some audit committees are beginning to use AI-enabled tools for summarization and issue tracking, with appropriate governance of confidentiality, retention, and validation.



What questions should the audit committee ask?

- What is management's process for identifying the highest priority topics for the audit committee's agenda over the next 6–12 months?
- How is management evolving its reporting to the audit committee, such as by incorporating dashboards and executive summaries without reducing transparency?
- What is management's process for implementing technology (including AI) to improve reporting and decision support? What governance is in place to support accuracy, confidentiality, and consistency?
- How is internal audit evolving its reporting to be more forward-looking to identify early-warning indicators, trend reporting, and thematic insights?
- How is the external auditor evaluating its communications and escalation process so the audit committee hears about issues earlier and with clearer context?
- What is the external auditor's process for aligning its work with that of internal audit to reduce duplication?



Where to go for more information:

[Year-end toolkit: Strengthening audit committee collaboration \(podcast\)](#)

[Audit committee effectiveness: practical tips for the chair](#)

[Audit committee dashboard reporting](#)

[Audit committee oversight checklist](#)

[Redefining internal audit oversight: strategies for audit committees](#)

[Oversight in the AI era: understanding the audit committee's role](#)

Connecting with the external auditor post-audit

What the audit committee needs to know

At this point in the annual cycle, the audit committee's oversight of the external auditor typically shifts from year-end audit execution, including the annual assessment of the audit firm, to reflection and forward-looking alignment. As companies continue to navigate the current business landscape, they face a variety of challenges that can impact their financial reporting, such as responding to geopolitical uncertainty and staying compliant with changing regulations. Connecting with the external auditor now can have many benefits, including a shared focus on emerging risks that may affect upcoming interim reporting and improved audit quality for the upcoming audit.

Restructurings and cost actions, impairment indicators, evolving contingencies, revenue changes, and tax matters can all introduce new judgment points and disclosure complexity. Similarly, shifts in systems, processes, or talent can change the internal control landscape. This is a good time to confirm that the external auditor's view of risk is anchored in the company's current environment.



Why is it relevant to the audit committee?

Oversight of the external auditor is a key component of the audit committee's role in supporting the integrity of financial reporting. When the audit committee surfaces learnings from the external audit early in the year and resets expectations, it reinforces the auditor's accountability to the audit committee, improves transparency, and creates a shared understanding of what is expected from both parties.

Just as importantly, the audit committee can use this time to connect audit oversight to the company's broader risk environment and pressure-test the company's readiness for the next reporting cycle. As business models continue to evolve and financial reporting processes become more technology-enabled, risk often shifts to data, systems, oversight, and documentation. Conversations with the external auditor now can help clarify where the auditor is seeing the greatest pressure points—whether in controls, estimates, disclosures, personnel, or the quality of management's support—and what the company can do to strengthen those areas. At the same time, the audit committee should share its perspectives on risk, including fraud risk, as the audit committee's perceptions of the risk landscape are integral to the external auditor's considerations of the risk environment.

What questions should the audit committee ask?

- Where did the external audit team encounter the most difficulty—whether in controls evidence, data quality, or management’s support for key judgments?
- Which areas does the external auditor expect will be higher risk in the coming year, and how will that change scope, interim work, or specialist involvement?
- Where does the external auditor anticipate potential disclosure pressure points in the next two quarters?
- What areas, if any, has the external auditor identified as having an increased risk of fraud?
- How does the external auditor expect its team to change in the current year and how will the team manage the transition?
- How has the external auditor considered the impact of emerging standards and regulations, geopolitical developments, and other matters on the company’s financial statements?
- What changes has management made to systems, processes, or people that could affect internal controls?



Where to go for more information:

[Overseeing the external auditors](#)

[Audit committee oversight checklist](#)

[Audit committee effectiveness: practical tips for the chair](#)

Understanding the SEC's potential shift to semi-annual reporting

What the audit committee needs to know

Recent public statements and market commentary suggest the SEC is actively considering a rulemaking initiative that could allow (or require) domestic registrants to move from the current quarterly Form 10-Q cadence to a semi-annual reporting framework. While no final proposal has been issued yet, the direction of travel has been reinforced by public remarks attributed to SEC leadership and by a **formal rulemaking petition** requesting the SEC to amend Exchange Act periodic reporting requirements to permit semi-annual reporting while maintaining timely Form 8-K reporting for material events.

Key benefits that have been cited for a change to permit semi-annual reporting include:

- Reduced costs and regulatory burdens, particularly for smaller firms
- Encouraging a long-term focus by reducing pressure on management to meet near-term, quarterly earnings targets
- Fostering capital markets by reversing the decline in public companies
- Providing market-driven flexibility by allowing companies to choose a reporting cadence that suits their business model
- Aligning US standards with international markets, such as the UK and EU, where semi-annual reporting is common



I thank President Trump for his idea of semi-annual reporting by public companies. The staff is currently preparing recommendations for each of these topics, and I eagerly await the commission's proposal for each recommendation."

—Paul S. Atkins, Chairman,
US Securities and
Exchange Commission

Even in a semi-annual reporting regime, the market should expect that material information would still need to be disclosed on a current basis (e.g. Form 8-K triggers, Regulation FD considerations), and many companies would likely continue some form of voluntary quarterly communications (e.g. earnings releases, investor decks) depending on, among other things, investor expectations, debt covenant requirements, and peer practices.

Why is it relevant to the audit committee?

A change in SEC reporting cadence—if proposed and ultimately adopted—could create both opportunity and risk. On the opportunity side, fewer required quarterly filings could reduce certain compliance burdens and give management more flexibility to focus on longer-term strategy.

On the risk side, the audit committee would want to:

- Confirm that any reduction in mandated periodic reporting does not inadvertently weaken transparency and consistency of disclosure through voluntary channels and that management confirms consistent messaging across channels
- Gain comfort that quarterly controls don't erode, even if SEC filing frequency changes
- Confirm processes remain strong so that any material developments are captured promptly via Form 8-K and other mechanisms
- Understand how the external auditor's approach (e.g. quarterly review procedures, interim testing) would evolve if the regulatory baseline changes

Now would be a good time for the audit committee to understand management's scenario-planning related to the potential change in reporting.

What questions should the audit committee ask?

- What is management's process for tracking potential SEC developments on semi-annual reporting, and what scenarios are being planned for (e.g. optional vs. required semi-annual filing; phase-in timing)?
- How is management considering investor, analyst, lender, or rating agency expectations in its scenario-planning?
- How is management tracking and considering potential changes in peer companies' reporting cadence?
- If the filing cadence changes, how is management determining which elements of the financial reporting process would remain quarterly and which would change?
- What is management's process for supporting continued strong disclosure controls and procedures for voluntary quarterly communications (e.g. earnings releases, investor decks) if the 10-Q cadence changes?
- How would the company's disclosure committee process change to see that material developments are still identified and disclosed promptly (including Form 8-K triggers and Regulation FD considerations)?
- If reporting cadence changes, what is internal audit's process for determining the areas with the greatest risk of control degradation, such as quarterly close controls, management review controls, and journal entry discipline?
- How would a move toward semi-annual reporting affect the external auditor's approach to quarterly review procedures, interim testing, and communications with the audit committee?



Where to go for more information:

[SEC to revisit quarterly reporting: Pros, cons, and what's ahead \(podcast\)](#)

[Financial reporting oversight](#)

Current considerations for internal audit oversight

What the audit committee needs to know

As the internal audit landscape continues to evolve, its functions are being asked to cover a broader set of enterprise risks—cybersecurity, third-party relationships, data governance, culture, and conduct—while still providing strong assurance over core controls and ICFR support. This can create pressure on capacity and prioritization. In response, some internal audit functions are adopting more flexible resource models, such as co-sourcing or targeted outsourcing to support peak workload periods (e.g. systems implementations) and to obtain specialized skills.

Internal audit teams are increasingly integrating AI-enabled tools into their work. In practice, this may include using AI to accelerate planning and risk sensing, analyzing large data populations for anomalies, drafting workpapers and reports, and supporting continuous monitoring. These capabilities can be valuable, but they also raise familiar questions in a new context: the quality of inputs, validation of outputs, documentation of judgments, and the need for clear accountability. Where internal audit relies on third parties for AI-enabled capabilities, the audit committee will want to understand governance, data handling, and documentation retention.

Further, many internal audit functions are updating how they ‘check controls.’ Traditional sampling-based testing remains important, but more internal audit teams are complementing it with data-driven assurance: automated tests, analytics, and continuous controls monitoring. That shift can produce earlier insights and broader coverage, but it also requires strong coordination with management and the external auditor.

Why is it relevant to the audit committee?

The audit committee's oversight of internal audit is to confirm the function is independent, appropriately resourced, risk-focused, and effective. A well-positioned internal audit function is often the audit committee's most reliable source of insight on whether the company's control environment is keeping pace with business change. This point in the calendar is an ideal time to confirm that internal audit's focus and methods remain aligned to the company's evolving risk profile—especially as change accelerates across technology, finance processes, and the control environment.

The audit committee will benefit from a focused conversation with internal audit on how it is managing a few key topics:

- Understanding how internal audit is maintaining a clear view of emerging risks and whether management's controls and governance are evolving with the risk landscape
- Maintaining a view on where controls are operating well and where design or execution gaps are developing—especially during transformations, reorganizations, or technology changes
- Confirming how internal audit is using technology to increase coverage and insight; understand where the company is undergoing change (e.g. systems, processes, people)
- Confirming internal audit has the right skills and capacity as well as whether co-sourcing or targeted outsourcing is appropriate to close gaps
- Supporting strong alignment among internal audit, management, and the external auditor to reduce duplication, focus assurance on what matters most, and help surface issues earlier
- Confirming internal audit's process for tracking remediation progress and validating that corrective actions are sustainable

In short, internal audit is not only a reporting function; it is a strategic mechanism for the audit committee to maintain confidence in controls, compliance, and operational discipline as the company changes.

What questions should the audit committee ask?

- How has internal audit's risk assessment changed since last quarter, and what are the top risks driving the plan this year?
- Where are the company's systems, processes, and people changing the most, and how is internal audit adjusting audit coverage in response?
- What is internal audit's process for integrating AI or advanced analytics into its work?
- How is the chief audit executive evaluating internal audit's skills, capacity, and technology to confirm it is appropriately resourced to cover emerging risk areas and core ICFR matters?
- What is internal audit's process for selecting and overseeing third-party providers?
- What is internal audit's process to confirm remediation is sustainable (e.g. clear ownership, timelines, testing, and reinforcement)?
- How is management using internal audit's insights to strengthen controls and risk management?
- What is management's process for identifying the most significant changes underway that could affect ICFR or compliance?
- What is the external auditor's process for coordinating with internal audit this year to avoid duplication and focus on the highest-risk areas?
- What leading practices is the external auditor seeing in the marketplace in terms of how internal audit functions are using analytics/AI, and which most improve audit readiness and control quality?



Where to go for more information:

[Oversight in the AI era: understanding the audit committee's role](#)

[Internal Audit at an inflection point](#)

[Redefining internal audit oversight: strategies for audit committees](#)

[Responsible AI and internal audit: what you need to know](#)

[Audit committee oversight checklist](#)

What the deals outlook could mean for audit committees



The 2025 M&A market was defined by AI-powered big deals. Looking ahead, we anticipate a more broad-based recovery as regulatory policy comes into focus and GDP growth expectations actualize, which will better position the middle market to actively participate in the M&A resurgence.”

—Kevin Desai, PwC US and Mexico Deals Leader

What the audit committee needs to know

After a few choppy years for transactions, the deals environment entering 2026 showed clearer signs of momentum, particularly for large, strategic transactions. **Megadeals rebounded in 2025** (with AI frequently cited as a strategic driver), even as parts of the middle market remained more subdued. However, that may change for the latter part of 2026 and beyond.

While each sector has its own dynamics, a few themes tend to recur in more active M&A cycles:

- Buyers often seek operating capabilities (data, AI, digital platforms, specialized talent) rather than just revenue growth, which increases reliance on valuation models, synergy assumptions, and integration execution
- Carve-outs and divestitures remain common, as companies attempt to reshape portfolios
- Speed and certainty are valued, resulting in compressed timetables—often putting pressure on diligence depth, accounting analysis, and financial reporting readiness

Why is it relevant to the audit committee?

The audit committee's role in deal transactions, such as mergers and acquisitions, has expanded from a traditional focus on financial statement risk to a more holistic, enterprise-wide oversight role. While the full board typically has ultimate responsibility for M&A strategy, the board increasingly relies on the audit committee's specialized financial and risk expertise to oversee transaction integrity, operational readiness, and post-close integration and synergy.

Deals can be value-creating, but they also introduce heightened risk to financial reporting quality, ICFR, and compliance. The audit committee plays an important role in confirming management's pace is matched by the rigor of accounting analysis, documentation, and controls. This may be a good time for the audit committee to refresh on its deals oversight role, which includes, among others:

- Confirming the integrity of financial reporting, internal controls, and enterprise risk management systems
- Supporting the company's compliance with applicable laws, regulations, and internal codes of conduct
- Confirming management maintains effective ICFR, assessing risk management frameworks, and oversight of internal and external auditors
- Acting as a key communications liaison, confirming that the interests of management, auditors, and shareholders are aligned
- Overseeing post-merger integration, including financial reporting integrity, internal control consolidation, and risk management



What questions should the audit committee ask?

- How does management characterize the current transaction pipeline, and what scenarios are most likely to move forward?
- What is management's process for determining the top financial reporting judgment areas a transaction would trigger (e.g. valuation, impairments, tax, revenue, contingencies)?
- What is management's process for identifying readiness gaps relating to financial reporting processes, data quality, controls, and disclosure discipline?
- What is management's process for confirming that ICFR keeps pace with deal activity—especially regarding systems changes, integration timelines, and segregation of duties?
- What is internal audit's process for factoring deal activity into its risk assessment and plan?
- How would internal audit coordinate with management and the external auditor to provide timely assurance without duplicating effort?
- If a capital markets transaction is undertaken, how would the external auditor stay aligned with the audit committee on emerging issues and escalation triggers?



Where to go for more information:

[Financial reporting oversight](#)

[Deals outlook 2026: Preparing finance teams for what's ahead \(podcast\)](#)

[US Deals 2026 outlook: The next wave of M&A: Bigger and bolder deals driven by AI and private equity](#)

Oversight of fraud risk

What the audit committee needs to know

Fraud risk remains a constant, but the ways fraud happens are changing. In today's environment, pressure points such as cost reduction, rapid growth initiatives, restructuring, and volatile markets can increase incentives and opportunities for misconduct. At the same time, the pace of change in technology—especially business transformation programs, automation, cloud migrations, and AI adoption—is reshaping the fraud risk profile in ways that can be easy to underestimate.

Two current shifts are particularly relevant:

Traditional schemes such as expense and procurement fraud, revenue manipulation, bribery/corruption, and misappropriation haven't gone away, but they are now frequently amplified by technology. Examples include social engineering (e.g. phishing emails), compromised credentials, payment diversion, and manipulation of digital approval workflows. AI can accelerate these threats by making impersonation more convincing and scaling the volume and sophistication of attacks (including deepfakes and realistic voice/video spoofing).

Digital transformation can create 'control gaps' if governance and controls don't keep pace. Large programs such as ERP implementations, shared services, system consolidations, new third-party relationships, and automation of finance and operations can temporarily weaken control discipline. Common vulnerabilities include access and segregation of duties, change management, overreliance on manual workarounds, and unclear accountability in newly redesigned processes—all of which can create ripe opportunities for fraud risk.

Why is it relevant to the audit committee?

Fraud risk oversight intersects with financial reporting integrity, internal control effectiveness, whistleblower programs, investigations, and auditor oversight. And it's important to note that from an audit committee perspective fraud risk isn't limited to financial statement fraud. Many fraud events can start as operational or cyber incidents and become financial reporting issues through loss recognition, contingencies, reputational impacts, or disclosure obligations.

The audit committee's role is twofold. It should have an understanding of and perspective on where fraud risk exists within the company. It should also confirm that the company has sound prevention, detection, escalation, and response capabilities, and that management's controls and ethics programs keep pace with how the business is evolving.

We offer a few techniques that can improve oversight without expanding meeting time:

- Request concise, periodic updates on fraud risk themes, emerging threats (including tech-enabled schemes), and control effectiveness, rather than a list of incidents
- Connect fraud risk to transformations by requesting a fraud lens in design decisions for major programs in areas such as access, approvals, data integrity, monitoring, and evidence retention
- Use internal audit to identify early-warning indicators, such as override trends, segregation of duties conflicts, and manual journal entry patterns
- Support compliance to surface hotline trends and culture indicators
- Confirm investigation governance is clear through, among other things, documented escalation processes and thresholds, engagement protocols for independent advisors, and maintaining attorney-client privilege

What questions should the audit committee ask?

- What is management's process for adjusting the company's fraud risk profile in response to business model and technology changes?
- What is management's process for identifying the company's greatest fraud risk exposure areas and how are emerging fraud risks identified?
- What is management's process for addressing tech-enabled fraud risks in policies, training, and verification procedures?
- How has management determined escalation triggers for potential fraud and how does management support timely and consistent decision-making?
- How does internal audit identify fraud risk themes that emerge from its work?
- What is internal audit's process for using data analytics to test for anomalies across large populations of information (e.g. payments, journal entries)?
- What is the external auditor's process for evaluating the effectiveness of the company's fraud-related controls and whistleblower processes?



Where to go for more information:

[Audit committee oversight checklist](#)

[Audit committee responsibilities](#)

[Global Economic Crime Survey](#)

[Overseeing internal investigations](#)

What a reconstituted PCAOB means for audit committees (and auditors)

What the audit committee needs to know

The PCAOB has entered a new chapter with a reconstituted Board appointed by the SEC on January 30, 2026. The SEC appointed Demetrios (Jim) Logothetis as Chair, and Mark Calabria, Kyle Hauptman, and Steven Laughton as new Board members, with George Botic continuing as a Board member (having served as Acting Chair until the new Chair was sworn in).

This leadership change follows a period of heightened attention on the PCAOB's direction, including how it balances investor protection with implementation cost and complexity for issuers and audit firms. In announcing the appointments, SEC Chair Paul S. Atkins emphasized a 'refocus' on the PCAOB's core statutory mission and a shift toward 'sensible, efficient oversight of auditors.'



While the new Board's full agenda will develop over time, two near-term implications are particularly relevant:

A likely recalibration of priorities and pace

The PCAOB has an active pipeline of standards and rulemaking initiatives. For example, the **PCAOB's new quality control standard, QC 1000**, has been adopted and approved by the SEC and is scheduled to become effective December 15, 2026—a milestone that will drive significant firm-level implementation activity and could influence how audit firms demonstrate and communicate audit quality. Going forward, the new Board may revisit how projects are sequenced, scoped, and operationalized—potentially changing timelines and focus areas that affect audit planning and execution.

A renewed emphasis on 'core audit quality basics'—including what inspection focus means for the audit

Regardless of policy direction, PCAOB inspections and enforcement continue to shape auditor behavior. Audit committees should pay attention to what the PCAOB signals as inspection emphasis areas and what auditors are doing in response—especially for recurring themes like significant estimates and judgments, internal control auditing, use of technology, and the rigor of audit evidence.

Why is it relevant to the audit committee?

The audit committee has primary oversight over the external auditor and is a key line of defense for audit quality. It is important for the audit committee to understand the potential implications of the shift in PCAOB leadership. The shift can influence audit firm behavior and the auditor's approach. Inspection focus areas, standard-setting priorities, and PCAOB enforcement posture can translate into changes in audit procedures, documentation requirements, and level of specialist involvement.

As auditors respond to changing PCAOB expectations and standards, management may see changes in requests for evidence, documentation of judgments, and engagement on controls and estimates. The audit committee will want to have transparent communications with the external auditor to confirm alignment on scope, key risks, and how emerging expectations will affect the audit plan.

What questions should the audit committee ask?

- What is the external auditor's process for determining how PCAOB developments are expected to influence the coming year's audit risk assessment, staffing, use of specialists, and communications cadence?
- Where does the external auditor expect the greatest changes in audit execution (e.g. timing, documentation expectations, and use of technology)?
- What is the external auditor's process for monitoring and identifying inspection themes that are most relevant to the company, and that could result in a change in audit procedures?
- How is management preparing for anticipated auditor requests for deeper or earlier evidence (e.g. significant estimates and judgments, controls documentation)?
- How is management evaluating and remediating changes in systems and processes that could affect ICFR and audit readiness this year?
- How is internal audit preparing to support audit readiness in the coming year?



Where to go for more information:

[PCAOB changes ahead: What they mean for auditors and preparers \(podcast\)](#)

[2025 AICPA & CIMA Conference: Current SEC and PCAOB Developments](#)

[Overseeing the external auditors](#)

Recurring items for the audit committee agenda

Every audit committee meeting agenda should include these important items or, at least, they should be discussed at scheduled intervals:

- Hotline complaints and code of conduct violations
- Changes in the regulatory environment
- Private and executive sessions
- Related-party transactions
- Internal and external audit plan reviews
- Discussions with the CIO, CISO, and GC as needed





To have a deeper discussion about how this topic might impact your business, please contact your engagement partner or a member of PwC's Governance Insights Center.

Contacts

Ray Garcia

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

Kathy Nieland

Partner, Governance Insights Center, PwC US
kathy.nieland@pwc.com

Gregory Johnson

Director, Governance Insights Center
gregory.johnson@pwc.com