

Your Q3 audit committee guide

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

September 2026



Table of contents

Topic 1	Financial reporting, compliance and disclosure considerations amid midterm election-year uncertainty	03
Topic 2	Reconnecting with the external auditor before year end	07
Topic 3	Impact of continued volatility on estimates and disclosures	10
Topic 4	Is the AI-enabled finance function ready for the year-end audit?	13
Topic 5	Cyber oversight in the age of AI and concentrated third-party technology risk	17
Topic 6	Internal audit oversight	21
Topic 7	Why readiness for California's new cybersecurity audit requirement starts now	24
Topic 8	Preparing for DISE implementation	28
Topic 9	Recurring items for the audit committee agenda	32

Financial reporting, compliance, and disclosure considerations amid midterm election-year uncertainty

What the audit committee needs to know

As the November midterm elections approach, companies are considering how potential changes in congressional priorities could affect tax, trade, federal spending, government contracting, industry regulation, and government oversight. Not every policy scenario will be material for every company. The objective for many companies will be to identify the limited number of plausible outcomes that could meaningfully affect the business and establish trigger points for action. Companies within certain industries could be more impacted than others, depending on how policy evolves. Some potential industries and impacts:

Private equity and healthcare: Continued scrutiny on private equity investments in specialized medical practices, elder care, and nursing homes may focus on how consolidation affects patient costs and care quality.

Energy and utilities: Traditional energy sectors and emerging artificial intelligence data centers may face pressure over power grid strains, local utility pricing, and environmental permitting rules.

Defense and national security: Private contractors and private equity firms active in defense supply chains may face heightened bipartisan and congressional committee oversight regarding foreign trade, pricing, and operational stability.

Housing and real estate: Residential homebuilding and corporate housing roll-ups are likely to remain central to political debates over living affordability and market consolidation.

Technology and digital assets: The pace of rulemaking on digital asset market structure rules, data privacy legislation, and AI infrastructure incentives may hinge on which party controls each chamber.

Policy uncertainty can affect assumptions underlying impairment analyses, valuations, tax positions, loss contingencies, liquidity assessments, and earnings guidance when it changes the company's expected business conditions. A company should develop scenario plans, when appropriate, that identify policy developments to be monitored, the assumptions or decisions that could change, the functions responsible for responding, and the circumstances that could require broader board attention.



Why is it relevant to the audit committee?

While public policy matters may not be under the oversight of the audit committee, the audit committee should understand where public policy uncertainty might intersect with compliance systems, internal controls, whistleblower processes, and public disclosures. The committee should assess whether management's scenarios are sufficiently company-specific and whether the financial statements, risk factors, MD&A, earnings releases, and investor communications tell a consistent story. And there is specific SEC guidance that requires a company to identify and analyze known trends and uncertainties that are reasonably likely to materially affect financial condition or operating performance.

The audit committee's role as it relates to potential policy changes is to understand whether election-related uncertainty is being appropriately considered in financial reporting, internal controls, compliance, and disclosures. For audit committees, the potential for tax accounting changes, regulatory enforcement shifts, and rules and regulations related to cybersecurity and AI oversight are key areas that should be on their watch list of matters that could be impacted by midterm election outcomes.



What questions should the audit committee ask?

- Which potential policy developments could have the most significant effect on the company's strategy, financial results, tax position, supply chain, or compliance obligations?
- How has management incorporated plausible election-related scenarios into forecasts and sensitivity analyses, and which assumptions are most exposed to change?
- What developments would trigger reassessment of significant estimates, capital allocation decisions, liquidity plans, or earnings guidance, and how quickly could management respond?
- What company-specific risks or known uncertainties may require updates to risk factors, MD&A, or other investor communications?
- How are political spending, lobbying, and trade association activities approved, monitored, and disclosed?
- How has internal audit considered election-year policy, compliance, and disclosure risks in its risk assessment and audit plan?
- How, if at all, does the external auditor expect policy uncertainty to affect its risk assessment, work on significant estimates, or year-end audit approach?



Where to go for more information

Tax policy, legislation, and regulations—including the 2026 midterm outlook

Tax policy outlook: What's on the horizon

How will US public policy shape business in 2026? (Podcast)

Reconnecting with the external auditor before year end

What the audit committee needs to know

Businesses are closing out the third quarter amid an operating environment that continues to be fluid. Changes in customer demand, interest rates, tariffs and supply chains, capital markets conditions, merger and restructuring activity, litigation, regulatory developments, and cyber incidents can affect forecasts, significant estimates, transactions, and disclosures. At the same time, finance transformation, workforce changes, outsourcing, and the growing use of AI are changing how financial information is produced, reviewed, and controlled.

From an external audit perspective, Q3 often marks the transition from planning to interim work to gear up for year-end execution. The auditor may be updating its risk assessment, completing or extending control testing, evaluating significant transactions and accounting judgments, coordinating specialists and auditors in other locations, and confirming staffing, timing, and information needs. Developments since the original audit plan was approved, such as a system implementation, acquisition, investigation, or change in key personnel, may require changes to the audit approach.

This makes late Q3 a natural time for the company and its external auditor to reconnect. Enough of the year has passed to identify how risks and judgments are developing, while time remains to address open matters before year-end demands intensify.

Why is it relevant to the audit committee?

The audit committee's fall agenda should include a refreshed external audit update that clearly distinguishes what has changed from the original plan. The update should cover emerging or heightened risks, interim work completed, significant accounting and disclosure matters, control observations and remediation, the involvement of specialists and other auditors, remaining milestones, management's audit readiness, and any expected changes in scope or fees. Potential critical audit matters and issues that could affect the timing of the company's annual 10-K filing should be discussed early rather than deferred until the audit is nearly complete.

Q3 is also a useful time to strengthen communication with the engagement team. A pre-meeting conversation between the audit committee chair and lead audit partner can help sharpen the formal meeting agenda. During the meeting, the committee can hear from key managers or specialists, assess the team's continuity, capacity, and industry knowledge, and obtain management's and internal audit's perspectives on coordination and performance.

Robust oversight leads to maximized value

Quality financial reporting is critical to the efficiency of the capital markets and protecting investors' interests. The audit committee's role in overseeing the external auditor and the company's financial reporting process is a key part of this. Building a strong relationship with the external auditor is vital and requires continuous communication, open and candid dialogue, and the ability to raise and address sensitive matters. Trust is the foundation.

The committee should also understand how the auditor is using or plans to use AI and other technology, the governance and human review supporting those tools, and how the company's own technology and finance-transformation initiatives are changing the audit. Our refreshed **Overseeing the external auditors** provides considerations for audit committees on AI and the external audit.

What questions should the audit committee ask?

- How has the external auditor's risk assessment and audit plan changed since the plan was initially approved, and what developments are driving those changes?
- Which significant transactions, estimates, accounting conclusions, disclosures, or control matters remain open, and what is the path to resolving them before year end?
- How are management, internal audit, and the external auditor coordinating on information requests, control remediation, audit readiness, and the reporting timetable?
- How does the engagement team's experience, continuity, workload, industry knowledge, and access to specialists support audit quality and timely execution?
- How is the external auditor using data analytics, AI, and other technology, and how are those tools governed, tested, and subject to appropriate human review?
- How are the company's use of AI, system implementations, outsourcing arrangements, and finance transformation activities affecting the auditor's approach and evidence needs?
- What changes arising from the auditor's implementation of the new quality control requirements or from firm inspection findings are most relevant to our engagement?

Where to go for more information



Overseeing the external auditors

Audit committee effectiveness: practical tips for the chair

Year-end toolkit: Strengthening audit committee collaboration (Podcast)

Impact of continued volatility on estimates and disclosures

What the audit committee needs to know

Volatility in trade policy, regulation, technology, supply chain, demand, financing, and geopolitical risk can quickly change forecasts and assumptions. For example, tariffs and potential tariff refunds illustrate how a public policy development can affect multiple parts of the financial statements. A company pursuing eligible refunds needs to support eligibility, preserve relevant rights, reconcile claims to customs and accounting records, evaluate the applicable accounting model, and update disclosures as facts change.

This means that a company should reassess sensitive estimates and disclosures, including asset impairment, inventory valuation, fair value measurements, credit losses, contingencies, tax positions, risk factors, and MD&A to confirm that their conclusions remain supportable and consistent across reporting.



Forecasts used in impairment testing should be consistent with budgets, tax projections, liquidity analyses, compensation plans, investor guidance, and other internal and external information. Disclosures should help investors understand material known trends and uncertainties, the reasons results changed, and the sensitivity of significant estimates when conclusions change. Risk factors, earnings materials, and other communications should align with financial statement assumptions and avoid presenting an incomplete or overly optimistic picture.

Why is it relevant to the audit committee?

Late Q3 is an important point for the audit committee to identify where management's judgments have become more difficult, which assumptions have changed since the prior year end, and where data or controls may be under pressure. Addressing these matters early can reduce surprises during the annual close and give the external auditor time to evaluate the supporting evidence.

The committee should obtain a focused view of the most sensitive estimates, including their magnitude, key assumptions, range of reasonably possible outcomes, changes from prior periods, management's use of specialists, and controls over source data, models, approvals, and disclosures.

Scenario and sensitivity analyses can be especially valuable. They can show how changes in demand, pricing, costs, currency, interest rates, or timing would affect an accounting conclusion, covenant, or liquidity forecast. They can also help the committee identify where management may need to update disclosures before the year-end reporting process is complete.

The audit committee should seek the external auditor's independent perspective on areas of heightened risk, contradictory evidence, the auditability of forecasts, and the quality of management's disclosures. Internal audit can complement that perspective by assessing the processes and controls used to generate key assumptions and by tracking the remediation of known deficiencies.

What questions should the audit committee ask?

- Which accounting estimates and disclosures have become more sensitive since the prior year end, and why?
- What assumptions have changed, and are those changes consistent across impairment models, budgets, tax forecasts, liquidity analyses, guidance, and compensation plans?
- What is the status of tariff refund claims or other recoveries, and how are eligibility, measurement, classification, and disclosure conclusions supported?
- Are inventory, supply chain, customer, or vendor developments creating new valuation, obsolescence, concentration, or continuity risks?
- How does the disclosure committee confirm consistency across the financial statements, MD&A, risk factors, earnings materials, and other public statements?
- What control deficiencies or process constraints could affect year-end estimates, and is remediation on track?
- Which areas does the external auditor believe are most likely to require additional evidence, specialist involvement, or committee attention?

Where to go for more information



Financial reporting oversight

Accounting implications of tariffs

Q2 2026 Closing statements: Quarter end insights for controllers

Is the AI-enabled finance function ready for the year-end audit?

What the audit committee needs to know

Although AI is increasingly embedded in finance and reporting workflows, AI adoption across financial reporting is not linear. Some companies may already use AI-enabled tools in the close, consolidation, reconciliation, forecasting, disclosure preparation, management reporting, control execution, or audit-support processes. Others may be conducting limited pilots or may not yet have implemented AI directly within financial reporting. AI may also enter the financial reporting environment gradually through third-party software updates, automation tools, analytics platforms, or informal employee use.



As AI adoption in the reporting process progresses, management should maintain an inventory of AI use cases that could affect financial reporting or ICFR. The inventory may capture the relevant business process, system or tool, owner, purpose, data inputs, degree of human involvement, implementation status, and potential relevance to ICFR. Because not all uses present the same risk, management should also classify them based on factors such as complexity, reliance on the output, data sensitivity, third-party involvement, and potential financial reporting or regulatory implications.

AI governance should be integrated into existing financial reporting and ICFR frameworks to support auditability. Where AI generates, analyzes, summarizes, or supports information used in the financial statements, disclosures, controls, or significant judgments, management should assess whether process narratives, flowcharts, risk-control matrices, and control descriptions need to be updated. Management should also define and document who reviews AI-assisted output, what evidence supports that review, how performance and exceptions are monitored, and when escalation or human intervention is required. Data quality, access, retention, confidentiality, vendor terms, and the availability of relevant third-party assurance information should also be considered.



Why is it relevant to the audit committee?

Oversight of a company's financial reporting is one of the audit committee's most critical responsibilities. Regarding the implementation of new technologies, the audit committee's role is to understand how management is pursuing innovation through a measured, risk-managed approach that preserves the reliability of financial reporting, the effectiveness of ICFR, data governance, documentation, and audit readiness. Regardless of the technology used, management remains responsible for the judgments, estimates, controls, and disclosures produced through the financial reporting process.

This becomes particularly important heading into year end. AI may affect how reconciliations are performed, journal-entry support is prepared, variances are investigated, estimates and forecasts are developed, or disclosure language is drafted. Although greater automation may help accelerate the close and reduce certain errors, the audit committee should still understand where overrides are possible, how exceptions are resolved, whether significant late adjustments were required, and how management confirms that AI-assisted analyses or disclosures are consistent with the underlying records.

As AI adoption increases, the external auditor may ask more detailed questions about where AI is used, how management assessed the related risks, how controls changed, and what evidence supports human review of AI-assisted outcomes. The audit committee should understand whether management can explain its higher-risk use cases and provide documentation supporting governance, validation, review, and control activities. Internal audit can also play an important role in assessing whether AI governance and controls are keeping pace with adoption and whether management is prepared for external auditor inquiries.

Now is the time for management, internal audit, and the external auditor to walk through the most significant AI-enabled processes. Early dialogue can clarify what evidence the auditor expects, whether controls are designed appropriately, and whether any process should be modified before the year-end close.

What questions should the audit committee ask?

- How has management identified where AI is currently being used, piloted, or contemplated in the close, consolidation, reconciliation, forecasting, disclosure, management reporting, or control processes—including AI embedded in third-party software and informal employee use?
- What inventory does management maintain of AI use cases that could affect financial reporting or ICFR, and how are those use cases risk-ranked?
- For higher-risk uses, how has management reassessed financial reporting risks and updated process narratives, flowcharts, risk-control matrices, control descriptions, or other SOX documentation?
- Who is responsible for reviewing and approving AI-assisted output, what evidence demonstrates that the review occurred, and what criteria trigger an exception, escalation, or human intervention?
- How does management validate the accuracy, completeness, reliability, and consistency of AI-generated analyses, calculations, summaries, or draft disclosures with the company's underlying books and records?
- How does management address data quality, access, confidentiality, retention, cybersecurity, and privacy risks, including restrictions on uploading sensitive information into external AI tools?
- How are AI-enabled features introduced by ERP, consolidation, close-management, or other software vendors evaluated, and do service organization reports or other assurance information address the relevant risks?
- What documentation and evidence does the external auditor expect regarding AI-enabled financial reporting processes, and are there any AI-related matters that could affect audit scope, timing, reliance on controls, or readiness for the earnings release and SEC filing?



Where to go for more information

[Financial reporting oversight](#)

[Overseeing the external auditors](#)

[Disclosure committee essentials](#)

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

Cyber oversight in the age of AI and concentrated third-party technology risk

What the audit committee needs to know

Companies increasingly rely on cloud platforms, enterprise software, managed service providers, payment processors, identity platforms, and other third parties to support critical operations and financial reporting. As a result, cybersecurity of third parties in a company's ecosystem remains a business resilience, financial reporting, and disclosure matter. An incident or prolonged outage at a third-party provider can disrupt multiple business processes, affect internal controls, and create financial reporting or disclosure implications.

AI is also increasing the complexity of this environment. Threat actors are using AI to make phishing, impersonation, and other attacks more convincing and scalable. At the same time, technology providers are embedding AI into products and services, sometimes through routine updates. These changes can alter how a company's data is used, how decisions are made, and how controls operate without being treated as a separate technology implementation.

Concentration risk may also be difficult to see. Several critical processes may depend on the same provider, while seemingly unrelated vendors may rely on a common cloud platform, identity provider, AI model, or other fourth party. As a result, traditional vendor due diligence, such as onboarding questionnaires and annual reviews alone, may not be sufficient. Management's approach should address the full vendor lifecycle—including risk tiering, due diligence, contractual protections, ongoing monitoring, incident response, resilience testing, and exit planning.

Why is it relevant to the audit committee?

Audit committees with responsibility for cybersecurity oversight should understand whether management has an effective, risk-based process for identifying critical providers, understanding shared dependencies, monitoring changes in risk, and escalating significant issues. The committee should also understand which providers support financial reporting or ICFR and how vendor-related risks are coordinated across cybersecurity, procurement, legal, finance, business continuity, and internal audit.

64% of S&P 500 companies disclose that the audit committee is responsible for cybersecurity oversight

Source: CAQ, Audit Committee Transparency Barometer 2025, December 2025.



At an upcoming meeting, the audit committee should request a focused view of the company's most critical technology-enabled services and the third parties supporting them. Reporting should highlight matters such as significant concentration exposures, shared fourth-party dependencies, high-risk findings, recent incidents, and the status of resilience testing. The objective is to understand changing exposure and unresolved issues as part of vendor assessments.

Over the near term, the committee should confirm that critical providers are included in incident response and business continuity exercises and that third-party incidents are integrated into the company's financial reporting, materiality, and disclosure processes. Management can use contract renewal periods to strengthen incident notification, information sharing, AI and data use, recovery protocols, and exit provisions. Internal audit can support by providing assurance over the completeness of vendor inventory, risk-tiering decisions, ongoing monitoring, and remediation. For providers relevant to financial reporting, management and the external auditor should also consider SOC report exceptions, subservice organizations, and complementary controls the company is responsible for operating.



What questions should the audit committee ask?

- How does management identify and prioritize critical third parties based on operational impact, data access, financial reporting relevance, and the availability of alternatives?
- Which critical processes depend on the same provider or shared fourth party, and what would be the impact of a prolonged outage or compromise?
- How does management monitor critical providers between formal assessments, and what events trigger an immediate reassessment?
- What significant third-party findings, accepted risks, or contractual gaps remain unresolved, and who is accountable for addressing them?
- How does management identify and assess providers' use of AI, including changes in data use, system access, models, and subprocessors?
- Which critical providers have participated in recent incident response or business continuity exercises, and what improvements were identified?
- How is internal audit evaluating the design and operating effectiveness of the third-party risk management program?
- How is the external auditor considering relevant service organizations, SOC report exceptions, complementary user controls, and third-party incidents in its audit approach?



Where to go for more information

[The board's role in overseeing cybersecurity](#)

[2026 Cybersecurity Outlook](#)

[New world, new rules: Cybersecurity in an era of uncertainty](#)

Internal audit oversight

What the audit committee needs to know

Internal audit is being asked to do more in a business environment that is moving faster and becoming more complex. In addition to core assurance over controls and support for ICFR, many functions cover a broader set of risks, including cybersecurity, third-party relationships, AI and data governance, culture, conduct, and transformation-related change. They are also doing increasingly more advisory projects in support of organizational change. That broader remit can create real pressure on capacity, prioritization, and skill needs.

In response, many internal audit functions are evolving how they work. More teams are using flexible resource models, including co-sourcing or targeted outsourcing, to address peak workload periods or obtain specialized skills. Many are also integrating AI-enabled tools, analytics, and continuous monitoring into risk assessment, planning, testing, and reporting. Those shifts can improve coverage and timeliness, but they also raise practical questions around governance, quality of outputs, documentation, and accountability.

Internal audit may also be changing how it provides assurance. We have observed more functions complementing traditional sampling with data-driven approaches that can produce earlier insight and broader coverage.

The broader takeaway for audit committees is that internal audit is no longer just a checker of controls after the fact. When positioned well, it can help the audit committee see where governance, controls, and operational discipline may be under strain as the company changes.

Why is it relevant to the audit committee?

Oversight of internal audit is one of the audit committee's core responsibilities. The committee should be comfortable that the function remains independent, appropriately resourced, risk-focused, and effective. A strong internal audit function is often one of the audit committee's clearest sources of insight into whether the company's control environment is keeping pace with business change.

Now is a good point in the year to revisit internal audit's plan, capabilities, and resource model. Many audit committees have had enough visibility into the year to understand where risks have shifted, where major programs or organizational changes are putting pressure on controls, and whether internal audit's original plan still reflects the company's current risk profile. And, as more internal audit teams undertake more frequent risk assessment activities, resulting in changes to internal audit plans throughout the year, this is a practical time for recalibration. If applicable, the audit committee should focus discussions on coverage of transformation activities, use of analytics and AI, co-sourcing decisions, and whether internal audit is surfacing insights early enough to support action before year end.

This is also a good time for the audit committee to confirm it is receiving the right reporting from internal audit. Rather than relying only on routine status updates, audit committees can use this point in the calendar to ask for a more focused discussion of what has changed, what matters most now, and where management, internal audit, and the external auditor may need to align more closely.

What questions should the audit committee ask?

- How has internal audit's risk assessment changed since the start of the year, and where is it adjusting coverage?
- How does management identify significant changes that could affect ICFR or compliance?
- Does internal audit have the skills, capacity, tools, and sourcing model needed to cover emerging risks and core ICFR work?
- How is internal audit using AI, analytics, continuous monitoring, or third parties, and what governance supports those choices?
- How does internal audit confirm that remediation is sustainable, and how is management using those insights to strengthen controls and risk management?
- How are the external auditor and internal audit coordinating to avoid duplication and focus on the highest-risk areas?



Where to go for more information

[Risk assessment, reimagined](#)

[Audit committee oversight checklist](#)

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

[The end of traditional internal audit: Human-led, agent-powered](#)

Why readiness for California's new cybersecurity audit requirement starts now

What the audit committee needs to know

California's final privacy regulations, effective January 1, 2026, require certain businesses subject to the California Consumer Privacy Act (CCPA) to complete an annual cybersecurity audit. The rule casts a wide net, applying to businesses whose data-processing activities pose a "significant risk to consumers' security." This includes businesses that meet specified thresholds based on revenue derived from selling or sharing personal information, or a combination of gross revenue and the volume or type of personal information processed. See **Privacy becomes a cybersecurity imperative under California's audit rule** for detailed requirements.

For businesses with more than \$100 million in 2026 annual gross revenue that are subject to the requirement, the first cybersecurity audit must cover the period from January 1, 2027 through January 1, 2028 (as specified in the **regulations**). The business must complete its audit report and submit a certification of completion to the California Privacy Protection Agency (CalPrivacy) by April 1, 2028. That makes the remainder of 2026 an important readiness window.

The audit requirement goes beyond demonstrating that policies exist. The audit must assess the establishment, implementation, and maintenance of the cybersecurity program and must be performed by a qualified, objective, and independent professional, who may be internal or external. Findings must be supported primarily by evidence such as documents, testing, sampling, and interviews, rather than management assertions or representations.

The audit covers a broad range of practices, including authentication, access controls, encryption, data and system inventories, vulnerability management, third-party oversight, incident response, and business continuity and disaster recovery. An existing cybersecurity audit, assessment, or evaluation may be leveraged if it satisfies all of the California requirements, either on its own or through supplementation. A member of executive management who is directly responsible for cybersecurity audit compliance, has sufficient knowledge of the audit, and has authority to submit must certify completion to CalPrivacy.

Management should therefore be determining applicability, defining the audit scope, establishing the audit delivery model, selecting an auditor, mapping controls, identifying evidence requirements, and addressing gaps before the first audit period begins. Independence should also be evaluated early because individuals performing the audit cannot participate in certain activities they may later assess (e.g. self-review threat due to designing control activities that they then may audit). Effective preparation will likely require coordination among cybersecurity, privacy, legal, compliance, procurement, internal audit, and other business leaders.

Why is it relevant to the audit committee?

The regulations require an executive leader directly responsible for the cybersecurity program to certify that the company completed the audit; they do not prescribe a particular board-committee oversight model. Even so, the requirement may directly affect the audit committee's oversight of internal audit, the external auditor, compliance, the broader control environment, and, in many instances, cybersecurity and data privacy.

The audit committee will want to understand management's determination of scope and accountability, the approach used to select the independent auditor, and the process for escalating findings and monitoring remediation. The committee should also understand how internal audit can support readiness efforts as well as the potential implications for cybersecurity-related disclosures, incident-response processes, financial reporting risk assessments, and the external audit, when relevant.



What questions should the audit committee ask?

- What is management's process for communicating the status and results of the audit to the audit committee?
- How has management determined whether the company and its relevant legal entities are subject to the cybersecurity audit requirement?
- What needs to be completed before the company's first audit period begins (including identifying the auditor), and where does management see the greatest readiness risks?
- How are management's privacy and cybersecurity teams aligning data inventories, systems, third parties, and control activities to establish audit scope?
- How can existing internal audits, external assessments, certifications, and control testing be leveraged, and what additional work will be necessary?
- What implications, if any, does the external auditor see for the company's cybersecurity-related risk assessment, public disclosures, financial reporting controls, and audit plan?



Where to go for more information

California's new cybersecurity audit requirements – Are you ready? (Podcast)

Privacy becomes a cybersecurity imperative under California's audit rule

Cyber accountability is rising: Is your organization ready for California's new cybersecurity audit requirements?

Preparing for DISE implementation

What the audit committee needs to know

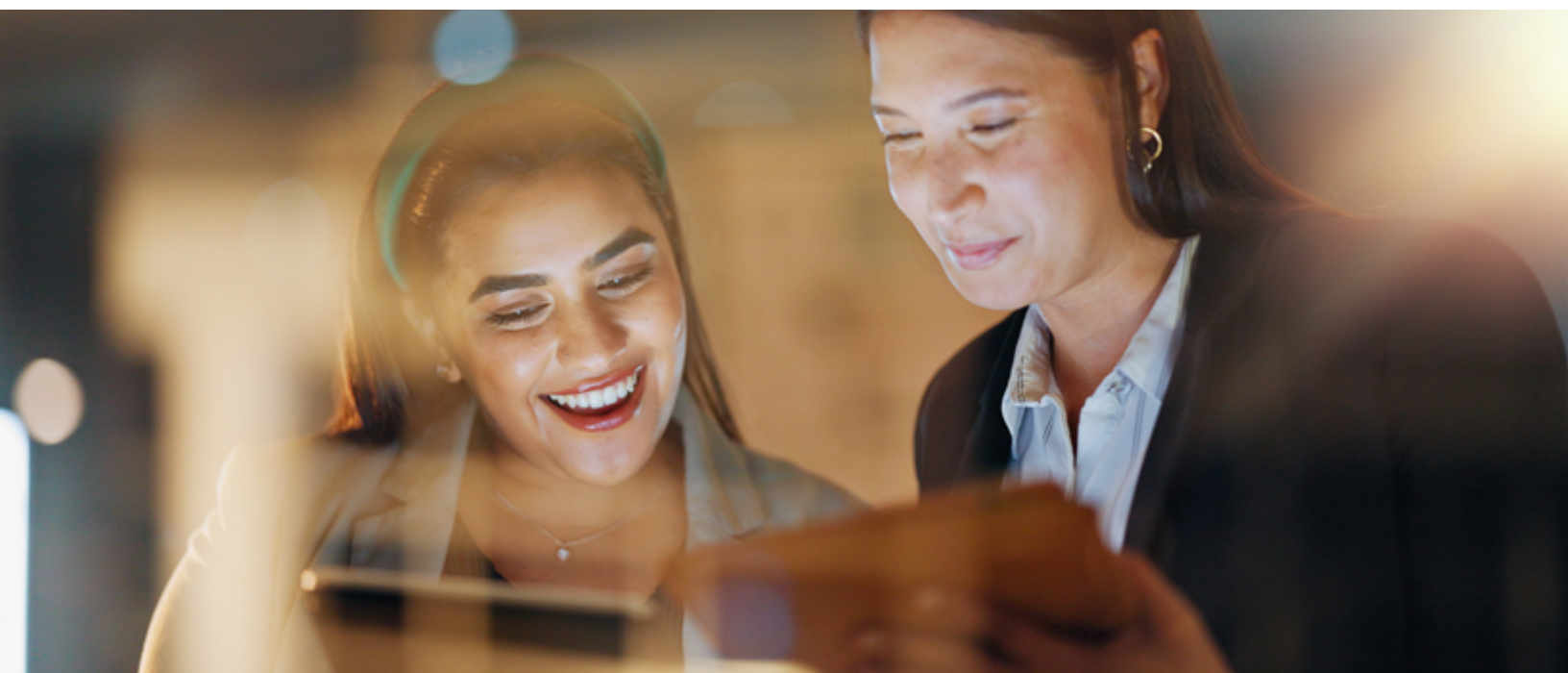
The FASB's disaggregation of income statement expenses standard, or DISE, will require public companies to provide more detail in the footnotes about the nature of expenses included in income statement captions. For audit committees, that means a disclosure change that could also affect systems, controls, and implementation planning. The standard takes effect for annual periods beginning after December 15, 2026, with interim reporting requirements beginning a year later. Early adoption is allowed, and a company can apply the guidance prospectively or retrospectively.

DISE at a glance

- New tabular footnote disclosure for relevant expense captions
- Required natural expense categories, including employee compensation, depreciation, intangible asset amortization, and purchases of inventory
- Qualitative explanation of amounts included in the 'other' category
- Separate disclosure of total selling expenses and, annually, the company's definition of selling expenses
- Effective for public companies in annual periods beginning after December 15, 2026, with interim requirements beginning a year later

In practical terms, the standard requires a new tabular footnote that breaks down relevant income statement captions into specified natural expense categories, including purchases of inventory, employee compensation, depreciation, intangible asset amortization, and depletion-related amounts. Within the same tabular disclosure, it also requires disclosure of certain expense, gain, or loss amounts that are already required to be disclosed under US GAAP, a qualitative explanation of what remains in the 'other' category, and separate disclosure of total selling expenses. The company's definition of selling expenses is required to be disclosed in annual reporting periods (or in interim reporting periods if the definition changed). DISE does not change how expenses appear on the face of the income statement, but it does give readers more visibility through the footnotes.

Those requirements may sound straightforward, but implementation could still take significant effort. Companies will need to understand what data is available, whether current systems can produce the required information, when estimates or other methods can be used to produce a reasonable approximation of the amounts required to be disclosed, and where controls may need to be designed and/or strengthened. They will also need to make practical judgments about which expense captions are relevant, how selling expenses should be defined, and whether existing reporting structures can support the required disaggregation for both annual and interim periods.



Why is it relevant to the audit committee?

DISE implementation includes inherent complexity as it touches more than disclosure. It may require management to revisit source data, reporting logic, control design, and governance over how expenses are classified, grouped, and explained. Further, it may require the use of estimates or other methods of approximation to derive amounts required for the disclosure. Because the audit committee oversees the quality and transparency of financial reporting, this standard deserves early attention.

The audit committee will want to understand whether management has identified the relevant expense captions, where existing systems can and cannot produce the required information, when estimates or other methods of approximation should be used, and whether added controls, documentation, or cross-functional coordination will be needed.

DISE may also shape the audit committee's interactions with internal audit and the external auditor. Internal audit can help assess readiness, governance, and whether new controls are designed and operating effectively. The external auditor can offer a useful perspective on tougher judgments, the strength of management's implementation plan, and areas where the new disclosures may attract added scrutiny.

More broadly, DISE may change how investors and other stakeholders evaluate operating performance by giving them more details about expense mix. That means the audit committee should think not only about technical compliance but also about whether the company communicates clearly, stays consistent with MD&A, and explains meaningful period-over-period changes once the new disclosures are required. For audit committees, a key takeaway is that DISE is not just a new disclosure requirement—it is also an implementation and oversight issue that warrants early attention.

What questions should the audit committee ask?

- What is management's plan for implementing DISE, and is the company on track for adoption?
- How is management determining which expense captions are in scope?
- What data gaps, system limitations, or process changes has management identified, and what is the plan to address them?
- How is management defining selling expenses, and what is driving that definition?
- How is management considering how the company's peers are thinking about defining selling expenses?
- How is management evaluating prospective versus retrospective adoption, and what would retrospective adoption require from a historical data and comparability standpoint?
- How will management confirm that DISE disclosures align with the company's broader financial reporting, including MD&A and other explanations of operating performance?
- How is internal audit assessing implementation readiness, and what role will it play in reviewing new or updated controls?
- What leading practices has the external auditor seen companies use to get ready for DISE adoption?



Where to go for more information

[Disaggregated expense disclosures: Don't roll the DISE \(Podcast\)](#)

[FASB issues new disaggregated expense disclosure requirements \(DISE\)](#)

[Financial statement presentation guide \(Chapter 3.11\)](#)

[Financial reporting oversight](#)

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





Contacts

Ray Garcia

Partner, Governance Insights Center Leader

ray.r.garcia@pwc.com

Kathy Nieland

Partner, Governance Insights Center

kathy.nieland@pwc.com

Gregory Johnson

Director, Governance Insights Center

gregory.johnson@pwc.com

Tracey-Lee Brown

Senior Director, Governance Insights Center

tracey-lee.y.brown@pwc.com