THE BULLETIN

Setting the 2025 Audit Committee Agenda

The next 12 months are likely to be another challenging year for audit committees. The 9 topics we have highlighted for 2025 may include some areas audit committees would consider beyond the official scope of responsibility as outlined in their respective charters. However, in recent years, many audit committees have experienced an expansion of scope and are being asked to provide oversight on a broader range of topics. If there is another board committee that has formal responsibility for any of the topics listed below, the audit committee should seek to collaborate and advise regarding the financial, reporting or internal control implications of such topics.

The 2025 Mandate for Audit Committees

1. Confirm that the committee is receiving adequate independent assurance regarding cybersecurity vulnerabilities.

2. Determine whether the organization is evaluating and capitalizing on generative artificial intelligence (GenAI) investments and opportunities responsibly.

3. Consider the maturity of the organization's governance over third-party relationships.

4. Validate that the committee's technology expertise enables effective oversight of technology-related risks.

5. Evaluate the strategy of the internal audit function to ensure that it is evolving at a pace that enables it to continue to add value to the organization.

6. Take a fresh look at the organization's current fraud exposure and the effectiveness of mitigation strategies.

7. Evaluate the organizational response to climate risk and other sustainability disclosure requirements.

8. Confirm the completeness and adequacy of the enterprisewide risk identification and management process.

9. Assess the effectiveness of management's reporting to the audit committee.

Face the Future with Confidence®

1. **Confirm that the committee is receiving adequate independent assurance regarding cybersecurity vulnerabilities.**

Audit committees should receive regular updates from those responsible for managing what has become many organizations' perennial top risk — cybersecurity. While this basic expectation is commonly fulfilled, audit committees must guard against being too eager to accept a report from the chief information security officer (CISO) highlighting only the positive actions being taken to protect an organization's assets.

Typically, effective governance would entail setting expectations of the internal audit function to provide independent assurance regarding the effectiveness of the people, processes and technology that have been put into place to manage cybersecurity risks. In practice, many internal audit organizations also rely on second-line actions or IT's engagement of a third-party assessor and may only be tangentially involved in scope-setting and issue follow-up. Many times this is because internal audit may lack the required skill sets to effectively perform the assessment itself or may not have the relationships needed to partner with IT to ensure that the proper levels of assurance are considered and achieved. Directors should regard this as a red flag.

Why it matters:

The costs of ineffectively managing cybersecurity risks are well documented. IBM's *Cost of a Data Breach 2024* report found that system complexity and skills shortages are amplifying breach costs globally to almost $5 million on average per incident.[1]

Key questions to ask:

—   How frequently is the audit committee briefed on cybersecurity-related risks, and who provides the updates?

—   Who determines the scope of independent assessments, and what is done to ensure transparency of results?

—   What coverage does internal audit provide over cybersecurity risks, and is the rationale for internal audit's coverage sound?

—   Are cybersecurity assessments covering both the design and operating effectiveness of critical technology controls across high-risk environments?

---

[1]   *Cost of a Data Breach Report 2024*, IBM.

2. Determine whether the organization is evaluating and capitalizing on generative artificial intelligence (GenAI) investments and opportunities responsibly.

The year 2024 has seen explosive growth in the utilization of AI by both individuals and corporations. While the overall adoption rate is high, the spectrum of where and how AI is being deployed within many organizations differs tremendously. Technology-centric organizations have made significant investments and are encouraging employees to leverage proprietary GenAI technologies. Less sophisticated organizations may leave it up to employees to tinker with broadly available, less secure tools. As regulators struggle to keep up and boards face challenges in knowing which questions to ask, a concerning gap may develop within many organizations.

While AI-aggressive entities might also take care to invest in appropriate governance structures to help manage opportunity and impact, this is not a given. Similarly, assuming that less aggressive organizations are not subject to significant risks resulting from employees' ad hoc utilization of AI tools is foolish. According to the Center for Audit Quality, 66% of survey respondents indicated their audit committee had spent insufficient time in the past 12 months discussing AI governance.[2]

Why it matters:

There are numerous data privacy and security-related concerns to navigate with AI usage, and regulatory scrutiny will catch up eventually. The committee must act to understand the organization's investments and adoption levels while considering the effectiveness of corresponding risk management activities to ensure responsible AI deployment.

According to the Center for Audit Quality, 66% of survey respondents indicated their audit committee had spent insufficient time in the past 12 months discussing AI governance.

---

[2] *Audit Committee Oversight in the Age of Generative AI*, CAQ, July 2024: www.thecaq.org/ac-oversight-in-the-age-of-genai.

Key questions to ask:

— Has the organization defined policies or a framework to govern the responsible use of AI?

— Has the organization defined a process, and does it have the capabilities, to track and monitor the use of AI throughout various departments and across the organization?

— Is an effective communications strategy in place regarding the organization's utilization of widely available GenAI tools?

— What investments are our primary competitors making regarding the use of AI-related technologies?

3. Consider the maturity of the organization's governance over third-party relationships.

According to Protiviti's 2024 Global Finance Trends survey, almost half of key critical finance and accounting functions such as accounts receivable, financial reporting, financial planning and analysis, and general ledger operations are performed by nonemployees.[3] Similar trends in IT and other operational areas have pushed an increasing amount of business responsibility outside of the well-vetted employee base. The utilization of domestic fractional labor pools, offshore and outsourced service providers, and other professional service relationships to address skill set and capacity challenges continues to become more generally accepted across all industries. Each of these staffing models presents various common and unique risks to consider, and most certainly broadens the purview of the control environment.

To the extent that third-party utilization has increased, the maturity of an organization's third-party risk management practices also needs to increase. Additionally, the more operationally critical the function, the more critical it becomes to have robust due diligence, contracting, onboarding, monitoring and offboarding procedures.

Why it matters:

The financial and operational impact of engaging with the wrong third parties can be devastating to the financial reporting process as well as to critical operating processes. Not having the appropriate contractual terms, service level agreements or monitoring capabilities may result in financial exposure at levels well beyond an acceptable appetite. Additionally, numerous cyber-related events have been sourced back to relationships with third parties that were not integrated into an effective governance structure.

---

[3] *Transform: Assessing CFO and Finance Leader Perspectives and Priorities for the Coming Year,* Protiviti, 2024: www.protiviti.com/sites/default/files/2024-09/2024_global_finance_trends_survey_protiviti.pdf.

Key questions to ask:

— What organizational trends are emerging regarding the use of third parties to support key management processes and controls?

— What key governance structures are defined and operating to manage the operational, cybersecurity, resilience, compliance, reputational, geopolitical and other risks related to third parties?

— To what degree are vendor management activities centralized or decentralized across various business areas, and what monitoring capabilities exist to identify new relationships (e.g., SaaS providers)?

— What contingency plans are in place if a key third party abruptly ceases operations or experiences a lengthy outage or ransomware event?

4. Validate that the committee's technology expertise enables effective oversight of technology-related risks.

According to the Corporate Governance Institute, 60% of directors do not believe their board has the skills or knowledge to effectively oversee the use of technology.[4] In today's digital world, every director should be technology-fluent, and a sufficient number of directors should be technology-savvy, with respect to key trends that will transform businesses — indeed, industries — in the very near future. Because fewer than half of boards conduct individual director assessments, the time has come for boards and audit committees to put a critical lens on technology skills and, if necessary, make the important changes needed to provide effective governance.

Why it matters:

In times of robust technological change and innovation, boards are a critical element to the overall governance structure, helping guide where investments are made and how risks are managed. The explosion of investment and adoption of cloud infrastructure, GenAI and quantum computing will continue to increase and may extend the knowledge gap between management and the board — unless appropriate steps are taken. Many of these large technology investments will support finance and accounting process transformations and materially impact operational processes. Investments made today may deliver operational efficiencies or customer-changing experiences that will materially impact organizational performance.

---

[4] "Adapt or Perish: Boards and Technology," by Dan Byrne, Corporate Governance Institute: www.thecorporategovernanceinstitute.com/insights/guides/boards-and-technology-adapt-or-perish.

> *With the broadening of internal audit scope into more operational areas, deeper knowledge of industry risks, emerging technologies and critical-thinking skills that bring an advisory mindset need to be cultivated.*

Key questions to ask:

— What technology expertise is present within the current committee composition, and what committee member experiences enable effective oversight of technology-related risks?

— Are the committee's technology-related experiences applicable and appropriate to current industry trends and future considerations affecting the company?

— What is the approach to rotating committee members and ensuring that new knowledge and expertise are brought to the committee with a regular cadence?

— Does the committee engage independent advisers for specific expertise (e.g., cybersecurity) when needed?

5. Evaluate the strategy of the internal audit function to ensure that it is evolving at a pace that enables it to continue to add value to the organization.

The audit committee should work with the chief audit executive and the chief risk officer (or its equivalent) to help identify the risks that pose the greatest threats to achieving business objectives. Internal audit is well suited to assist in many evolving areas, such as providing an internal control focus over shared services transitions or throughout system implementations. Other areas may require stretching of unused muscles, like supporting transaction readiness as merger and acquisition activities reaccelerate. While some activities may require consideration of adequate independence, the impact that internal audit can have on these types of engagements is undeniable.

As the scope of internal audit evolves, so do the required skill sets for auditors. Emphasizing continuous learning and development ensures that the team has the necessary expertise in areas such as data analytics, AI governance and cybersecurity. With the broadening of internal audit scope into more operational areas, deeper knowledge of industry risks, emerging technologies and critical-thinking skills that bring an advisory mindset also need to be cultivated.

Why it matters:

Audit committee members are well served to support and encourage internal audit strategy evolution in alignment with the organization's overall strategy.[5] If the strategy of the internal audit function does not continue to evolve in this manner, the value it can provide will be limited.

Key questions to ask:

— How does the current internal audit strategy align with the overall business strategy and objectives? How frequently is this alignment reassessed?

— What changes have been made recently to the audit strategy or plans to address emerging risks such as cybersecurity threats, technological advancements, regulatory changes or environmental, social and governance (ESG) considerations?

— What steps are being taken, and what ongoing training programs are provided, to ensure that internal audit personnel possess the necessary skills to handle evolving business complexities and risks?

— With the continued challenges in the labor market, does internal audit have the talent it needs? How do you know?

6. Take a fresh look at the organization's current fraud exposure and the effectiveness of mitigation strategies.

Various factors have resulted in corporations having to respond to new issues, such as employees working multiple (remote) jobs and engaging in "quiet quitting." One persistent challenge that has not gone away, but continues to evolve, is corporate fraud. While one could argue that remote work in a digital age has not created more *opportunities* for employees to commit fraud, perhaps the fraud triangle[6] element that has shifted the most in recent years is *rationalization*. Corporations have become a frequent target of politicians, social media and activists and are commonly characterized as "greedy," even when financial returns are modest. Perhaps now more than ever, the time has come for a robust and refreshed view of fraud possibilities within the organizations' virtual and physical walls. Moreover, turning the lens beyond employees to actively consider scenarios that include contractors, vendors or customers may reveal surprising results.

---

[5] 2024 Global Internal Audit Standards, The Institute of Internal Auditors: www.theiia.org/en/standards/2024-standards/global-internal-audit-standards.

[6] "Fraud 101: What Is Fraud?" Association of Certified Fraud Examiners: www.acfe.com/fraud-resources/fraud-101-what-is-fraud.

Why it matters:

Fraud is a common occurrence, and it's very possible that it is occurring within your organization right now. According to the 2024 *Report to the Nations*, released by the Association of Certified Fraud Examiners, thousands of frauds are committed costing corporations billions of dollars each year.[7] Fraud impacts the bottom line and, when continuing undetected, can spread as others observe the lack of internal control and monitoring.

Key questions to ask:

— Has management identified any cases of fraud in the last five years? If so, what lessons have been learned from these cases?

— Does the organization conduct a fraud risk assessment that engages appropriate leaders and involves various areas of the business to identify common fraud scenarios? Does the assessment consider the areas most susceptible to fraud?

— Are employee hotlines effectively implemented, publicized and monitored for responsiveness? Is the audit committee seeing the feedback received in an unvarnished manner?

— Does internal audit consider fraud as a part of its annual planning process and then again within each audit on the calendar?

Fraud impacts the bottom line and, when continuing undetected, can spread as others observe the lack of internal control and monitoring.

7. Evaluate the organizational response to climate risk and other sustainability disclosure requirements.

Despite the uncertainty regarding the U.S. Securities and Exchange Commission's proposed rules, existing regulations on the books such as the European Sustainability Reporting Standards (ESRS), the EU's Corporate Sustainability Reporting Directive (CSRD) and California's legislation require companies to disclose more detailed information on their climate-related impacts. Climate

---

[7] *Occupational Fraud: A 2024 ACFE Report to the Nations®*, Association of Certified Fraud Examiners: www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

change introduces new financial risks, including physical risks (e.g., extreme weather events) and transition risks (e.g., shifts in market preferences or regulatory landscapes). Most regulations include assurance requirements and indicate that certain reported elements will need to be audited in the future.[8]

Despite an extended time frame for the aforementioned regulatory requirements, processes to support anticipated disclosures need to be designed and implemented. Even smaller organizations not directly subject to current regulations are affected, as customers and vendors will ask them for information. And, significantly, companies voluntarily reporting this information — the overwhelming majority — need to ensure its accuracy, even though the disclosure itself is not required.

It is important for the audit committee to confirm that management is identifying skilled resources now who can become familiar with new materiality assessment requirements, especially those that call for analyses of impacts and risks that exist throughout the organization's carbon footprint and ecosystem. These resources should begin identifying the data that will be meaningful to report and designing processes for gathering information that will serve as a benchmark going forward.[9]

Why it matters:

Companies operating in the EU and in California must comply with their disclosure requirements, regardless of what happens to the proposed SEC rule. Noncompliance with evolving climate-related regulations can lead to significant legal penalties and reputational damage. Inaccurate voluntary reporting can have the same result. Investors are increasingly factoring climate risk criteria into their decision-making processes. Failure to effectively manage and disclose climate risks can result in reduced investor confidence and potentially lower stock valuations as well as cause brand and reputation damage and loss of market permission in certain markets.

Key questions to ask:

— How is the organization considering and responding to new disclosure requirements related to climate risks?

— Has the organization secured the necessary resources with relevant expertise to address additional reporting requirements and manage responses to shifting sustainability reporting viewpoints? How do you know?

---

[8] "GHG Emissions Reporting Considerations for Smaller Enterprises," by Mark Boheim and Jacob Chu, 2024, Protiviti: https://blog.protiviti.com/2024/08/29/ghg-emissions-reporting-considerations-for-smaller-enterprises.

[9] *Transform: 2024 Global Finance Trends Survey Report,* Protiviti, September 2024: www.protiviti.com/sites/default/files/2024-09/2024_global_finance_trends_survey_protiviti.pdf.

— Have business-continuity plans been updated to address potential disruptions from climate-related events?

— How does the organization communicate its climate risk management strategies to stakeholders, including investors, customers and employees? What feedback mechanisms are in place to gauge stakeholder perceptions of the organization's environmental responsibility efforts?

8. Confirm the completeness and adequacy of the enterprisewide risk identification and management process.

Risks are evolving more quickly in a business environment marked by rapid technological advancements and geopolitical uncertainties, necessitating robust enterprise risk management (ERM) practices that ensure timely identification of and responses to dynamic risks. The audit committee should understand management's processes to assess risks and determine whether action plans mitigate risks to acceptable levels. The increasing complexity and interconnectedness of risks have prioritized more holistic risk management and oversight. Many (if not most) audit committees today are shouldering heavy risk agendas and oversight responsibilities beyond their core responsibilities — for cybersecurity, ESG and regulatory compliance risks, as well as oversight responsibility for all of, or aspects of, management's ERM system and processes.[10]

Why it matters:

Effective audit committee oversight of the organization's holistic risk management, on its own or in collaboration with other committees of the board or the full board, can enhance the committee's effectiveness in discharging its oversight responsibilities in other areas. It also can result in improved relationships with investors, regulators, customers, employees and other stakeholders.

Risks are evolving more quickly in a business environment marked by rapid technological advancements and geopolitical uncertainties, necessitating robust ERM practices that ensure timely identification of and responses to dynamic risks.

---

[10] "2024 The State of Risk Oversight: An Overview of Enterprise Risk Management Practices — 15th Edition," Enterprise Risk Management Initiative at NC State University, July 23, 2024: https://erm.ncsu.edu/resource-center/the-state-of-risk-oversight-an-overview-of-enterprise-risk-management-practices-15th-edition.

Key questions to ask:

— Are adequate resources deployed to the ERM process to handle ever-expanding risks?

— Would individual audit committee members be able to consistently describe management's risk management process?

— How does the committee (and other board committees and/or the full board) evaluate the completeness of management's assessment of the company's top risks against external sources?

— If there has been a recent unforeseen event, did our postmortem identify the need for necessary updates to the organization's ERM processes?

9. Assess the effectiveness of management's reporting to the audit committee.

It is crucial that management — and internal audit — provide high-quality and concise information with the right context, rather than disparate data points, to the audit committee. The role of an effective audit committee demands an enterprisewide, big-picture view rather than reporting from multiple parties and silos to identify potential blind spots.[11] The audit committee should request collaboration from board-facing members of management and internal audit to ensure that the reporting the committee receives is succinct, strategically relevant and actionable. Board materials should not force an administrative reconciliation exercise on directors.

Why it matters:

Oversight responsibilities continue to broaden for many audit committees, requiring relevant and easy-to-digest information that supports effective governance. Holistic reporting to the audit committee of common themes identified by internal and external assurance providers supports the audit committee in discharging its chartered responsibilities. With the ever-increasing pace of change, it is critical that management reporting supports effective and focused audit committee oversight and continued alignment of organizational and internal audit resources.

---

[11] "Blind Spots in the Boardroom," *Board Perspectives*, Issue 170, 2023, Protiviti: www.protiviti.com/us-en/newsletter/bp170-blind-spots-boardroom.

Key questions to ask:

— Do management reports stimulate thinking, facilitate learning and draw out the best advice from the audit committee? If not, what improvements are needed?

— How can cross-functional communication with the audit committee be facilitated among departments such as finance, compliance and operations to ensure cohesive summations from management?

— When appropriate, does management reporting integrate internal and external sources of assurance regarding the organization's risks?

— What mechanisms are established for collecting feedback from directors regarding the quality of communications and reports they receive, including context, data visualization and brevity?

Self-Assess Committee Effectiveness

Audit committees are encouraged to self-assess their performance periodically. To that end, we have made available illustrative questions at www.protiviti.com/us-en/newsletter/bulletin-assessment-questions-audit-committees. Committee members should periodically assess the committee's composition, charter and focus with consideration of the company's industry, circumstances, risks, financial reporting issues and current challenges.

Topics Covered by "Assessment Questions for Audit Committees to Consider"

- Committee composition and dynamics
- Committee charter and agenda
- Oversight of internal controls and financial reporting
- Oversight of the external auditor
- Risk oversight
- Business context

- Corporate culture
- Executive sessions
- ESG reporting
- Oversight of the finance organization
- Oversight of internal audit
- Committee effectiveness
- Member orientation and education

About the Authors

Andrew Struthers-Kennedy
Protiviti Managing Director
Global Practice Lead, Internal Audit and Financial Advisory

As the global lead of Protiviti's Internal Audit and Financial Advisory practice, Andrew Struthers-Kennedy is privy to significant boardroom experience — his own as well as that of the managing directors he leads. His market focus is on increasing the relevance of and value delivered by internal audit both in the boardroom and across the company.

Gordon Braun
Protiviti Managing Director

Gordon Braun is in Protiviti's Internal Audit and Financial Advisory practice and has more than 25 years of experience. Gordon focuses on engagement with chief auditors, executives and board members on topics such as governance, risk management and oversight (including related to emerging risks), and strategy and transformation of internal audit and enterprise control programs.

Kristen Kelly
Protiviti Director

Kristen Kelly is in Protiviti's Internal Audit and Financial Advisory practice and has nearly three decades of experience. Kristen is heavily involved in many of our thought leadership efforts, with a primary focus on chief auditors and board members on topics such as internal audit professional standards and leading practices, Sarbanes-Oxley compliance and risk management.

Acknowledgements

protiviti ®