WHITE PAPER

Setting the 2026 Audit Committee Agenda

Key Focus Areas for the Year Ahead

protiviti®
Global Business Consulting

2026 promises to be another year of increasing demand for audit committee members. Some of the nine topics we have highlighted for this year's agenda reflect a growing array of responsibilities that may extend beyond traditional boundaries. As oversight expectations continue to evolve, many audit committees are being called upon to engage with broader enterprise risks and governance matters. Risks, spanning cyber, AI, talent and third parties, among others, are also becoming increasingly interdependent, requiring organisations to remove silos and adopt integrated strategies for holistic assessment and management.

The 2026 Mandate for Audit Committees*

1. Understand technology's impact on the control environment.
2. Reevaluate management's governance structure.
3. Keep pace with cybersecurity and data privacy risks.
4. Ensure balance between AI governance and AI investment.
5. Assess organisational talent and capabilities to innovate and address uncertainty.
6. Align on regulatory risk tolerance.
7. Assess culture as a mechanism to drive ethical behaviour.
8. Evaluate audit committee expertise and composition as expectations expand beyond financial reporting.
9. Understand and support internal audit's reinvention for the future.

* Audit committees are encouraged to self-assess their performance periodically. As a companion piece for this mandate, we have made available illustrative self-assessment questions.

1. Understand technology's impact on the control environment.

Many major companies are planning significant layoffs in the coming year as a direct consequence of their artificial intelligence (AI) implementations. It's a reasonable bet more will follow, across most industry sectors, as organisations continue to reevaluate the size and composition of their teams in the AI era. These moves reflect a broader trend toward automation and digital transformation, with many organisations restructuring their workforces to embrace new technologies and remain competitive.

AI-driven layoffs and workforce transformations can have a profound impact on the effective operation of established internal controls. The risk is that, in planning AI initiatives, those controls may become an afterthought. This issue goes beyond managing the risks directly associated with AI and maintaining a "human in the loop." While AI may automate certain processes and even strengthen some controls, it can introduce new risks or weaken existing controls — such as segregation of duties — particularly during workforce reductions and organisational changes.

Audit committees should ensure that the chief financial officer (CFO), chief audit executive (CAE), chief information officer (CIO) and others are advocating for sustaining the control structure throughout AI planning and implementation.

Other technology initiatives, including modernisation efforts meant to address technical debt, will also affect the control environment — potentially for the better. Many organisations now operate within an evolving technology ecosystem, often shaped by mergers and acquisitions, comprising multiple enterprise resource planning (ERP) systems, human resources information systems (HRIS), customer relationship management (CRM) tools, and operational technology environments. Widespread reliance on third-party relationships and fresh cybersecurity risks emerging from technology deployments are also key considerations.

The bottom line is that technology changes will have a significant impact on key internal controls.

Why it matters

As companies accelerate AI adoption and technology modernisation, the design and effectiveness of internal controls will increasingly determine whether these changes strengthen or destabilise their operations. Automation can greatly enhance efficiency, but overlooking control implications during transformation can expose companies to operational errors, fraud risk or compliance gaps. Audit committees that stay ahead of these shifts — by insisting on clear accountability, robust governance and proactive evaluation of controls — can help ensure technology investments increase resilience rather than erode it.

Key questions to ask

- How are emerging technologies, such as automation, AI and cloud platforms, changing the design and effectiveness of our internal controls—and are the appropriate executives advocating for sustaining the control structure during implementation planning?
- Where might we have weaknesses in our control environment due to overreliance on outdated technology or failure to account for implementation risks?
- Is the committee receiving assurance regarding technology modernisation and AI implementations to avoid blind spots in the control environment?

2. Reevaluate management's governance structure.

Audit committees play a critical role in ensuring that an organisation's governance structure is not only well designed but also effectively executed. A key part of this oversight involves evaluating whether the Three Lines Model — including risk owners, risk managers and internal audit — is delivering the intended benefits of accountability, transparency and resilience in an era of unprecedented change.

While the Three Lines Model is widely recognised, implementation often falls short. Many organisations struggle to define boundaries between the lines or adopt siloed approaches that hinder collaboration and timely information sharing. Known issues may not be communicated promptly for effective remediation. Other challenges include cultural resistance, poor integration with governance processes and competing priorities that limit resources. These issues can lead to duplicated efforts or unnoticed gaps in coverage.

Technology advancements are helping to improve coordination of efforts and address issues that were previously difficult to manage. Outdated methods supported by spreadsheets and email are increasingly being replaced, but the sheer number of governance, risk and compliance (GRC) software solutions — ranging from broad enterprise platforms to niche tools — creates a complex selection landscape that can frustrate stakeholders.

Centralising risk data through a GRC system can drive a common nomenclature and provide enhanced visibility into risk trends, while workflow automation helps route the right information to the right people at the right time. However, adoption and full implementation are often uneven, and partial rollouts can leave some of the most desired benefits out of scope or deferred for future phases.

In any case, audit committees should encourage management to periodically evaluate existing tools and explore new ones that can help close gaps and strengthen coordination across the responsible departments. They should also be proactive in assessing whether the Three Lines Model is supported by the right tone, structure and resource allocation to enable responsive governance. Determining where gaps may exist will help drive meaningful change that supports the achievement of organisational objectives in challenging times.

Why it matters

As organisations adapt to rapid technological, regulatory and market changes, strong governance can keep strategy and oversight aligned. Without clear accountability among the three lines, or effective systems to support coordination, critical risks can go unnoticed until they evolve into material issues. A well-functioning governance structure can empower both risk owners and internal audit, creating a feedback loop that helps increase resilience, transparency and stakeholder confidence.

Key questions to ask

- Do the roles and responsibilities across the three lines clearly align and operate without duplication or gaps in coverage?
- Is there sufficient transparency and communication among the three lines to ensure timely escalation of risks and alignment with strategic objectives and regulatory expectations?
- Does the audit committee receive consolidated or coordinated risk reporting from each of the three lines?

3. Keep pace with cybersecurity and data privacy risks.

As AI and other technologies amplify both the scale and sophistication of attacks, audit committees must sharpen their oversight of cybersecurity and data privacy risks. Traditional governance models and control frameworks struggle to keep pace with the velocity of change, and the proliferation of data — along with its frequent transmission to and from third parties — creates an environment ripe for exploitation. For the second straight year, CFOs responding to Protiviti's Global Finance Trends Survey cited security and privacy as their top concern.[1]

Yet many boards overestimate their preparedness. A recent *Harvard Business Review* study found that while most executives believe cyber funding is adequate, only a minority view their boards as proactive or innovative in managing cyber risk.[2] Indeed, cybersecurity failures can often expose shortcomings in boardroom oversight. Post-incident board debriefing sessions can reveal gaps in expertise, questions that went unasked and assurance methods that were never pursued.

1 *2025 Global Finance Trends Survey Report*, Protiviti, Sept. 2025.

2 "Boards Need a More Active Approach to Cybersecurity," by Noah P. Barsky and Keri Pearlson, *Harvard Business Review*, May 20, 2025.

New, AI-amplified threats are exacerbating these issues and widening the knowledge and capability gap. Bad actors can now deploy techniques such as data poisoning, model inversion and automated prompt injections for faster, more scalable attacks — alongside more targeted methods leveraging deepfakes or spear phishing. A recent Accenture report found that 90% of organisations lack the maturity to defend against AI-enabled threats, and also that only 36% of technology leaders recognised that generative AI was outpacing their security.[3] If technology leaders have a blind spot, the challenge for committee members is undeniable.

Audit committees should probe technology leadership regarding unaddressed risks and deferred investments and partner with risk management functions to better understand known vulnerabilities and areas lacking control assurance. Requesting more refined, data-driven reporting on how assurance is achieved — and where audit coverage may be insufficient — can help enable robust conversation and strengthen overall risk alignment and oversight.

Why it matters

Cybersecurity and data privacy risks, which have been exacerbated and complicated by the expansion of third-party ecosystems, have become central to enterprise resilience and board accountability. As AI accelerates innovation as well as risk exposure, oversight that once centred on compliance must evolve toward strategic assurance — probing how management anticipates, mitigates and communicates emerging vulnerabilities, including those in third-party environments. An informed and engaged audit committee can help ensure appropriate investment in cyber defences, reinforce accountability and set a tone of vigilance and transparency from the top.

Key questions to ask

- What emerging cybersecurity and data privacy risks, particularly those amplified by AI, are beginning to impact the organisation, and how is the committee obtaining assurance regarding the company's risk mitigation activities?
- How is the company evolving its cybersecurity and data governance strategy to anticipate and respond to future regulatory expectations and technological advancements?
- Has the maturity of the company's third-party risk management program increased commensurately with reliance on third parties to support business processes and technology?

[3] *State of Cybersecurity Resilience 2025,* by Paolo Dal Cin, Daniel Kendzior and Yusof Seedat, Accenture, June 25, 2025.

4. Ensure balance between AI governance and AI investment.

Generative and agentic AI are reshaping operating models and heightening the need for assurance, elevating both the need for accountability and the opportunity for innovation. The *2026 Global Risk in Focus* report from The Institute of Internal Auditors (The IIA) shows digital disruption (including AI) surging into the top five risks across all regions, driven by rapid generative AI adoption and AI-enabled cyber threats. Boards are increasingly expecting management to form dedicated AI governance teams, while internal audit functions are expanding their own use of AI to enhance efficiency and coverage.[4]

The audit committee should understand management's dual mandate: instituting robust governance to manage model risk, data integrity, ethics and regulatory compliance, while simultaneously avoiding strategic obsolescence by investing in AI capabilities.

The number of organisations using AI in finance increased from 34% in 2024 to 72% in 2025. However, of the 72%, only 27% are doing so pursuant to a control plan.[5] NAVEX findings highlight key governance gaps — including policy ownership skewed toward IT, visibility issues and insufficient AI training — underscoring the need for integrated governance and sustained board engagement.[6] Only one-quarter of organisations have fully implemented AI governance, while 44% cite unclear ownership as the leading obstacle to AI governance.

[4] *2026 Risk in Focus: Hot topics for internal auditors*, The Institute of Internal Auditors (The IIA) and the Internal Audit Foundation, 2025.

[5] *2025 Global Finance Trends Survey Report*, Protiviti, Sept. 2025.

[6] *State of Risk & Compliance Report*, NAVEX Global, 2025.

Without clearly defined roles, formalised handoffs and coordinated processes between technical and risk functions, organisations are left with what might be called "distributed responsibility without distributed accountability." And in a field as fast-moving and high-stakes as AI, that's a serious structural vulnerability.[7]

A practical governance approach often begins with a cross-functional AI council (IT, compliance, legal, risk, data privacy, internal audit, etc.) that defines strategy, policies, roles and responsibilities, escalation paths, life cycle controls, and ownership.[8] Organisations should embed AI risk management within the enterprise risk management (ERM) framework and the Three Lines Model:

- **First line:** designing and operating controls
- **Second line:** monitoring AI risks (e.g., bias, privacy, cyber)
- **Third line:** providing independent assurance and model validation where needed

The audit committee's oversight should explicitly include compliance with evolving AI and privacy regulations, the organisation's use of AI in finance and internal audit, and the internal controls supporting AI-related disclosures and data governance.

Why it matters

AI is redefining how companies create value — and manage risk. The pace of innovation is outstripping traditional mechanisms for oversight, making it essential for boards to align AI investments with sound governance. When audit committees insist on clarity of ownership, robust control design, and transparency around model performance and ethics, they can help ensure that AI delivers measurable business advantage without compromising integrity, compliance or stakeholder trust.

Key questions to ask

- How has the organisation defined and clarified ownership for AI governance?
- Is the organisation balancing innovation and accountability to stay competitive amid the accelerating shift from generative to agentic AI?
- What frameworks are being used to help ensure responsible deployment without stifling innovation?

[7] *From Blueprint to Reality: Execute Effective AI Governance in a Volatile Landscape*, AuditBoard, 2025.

[8] Ibid.

5. Assess organisational talent and capabilities to innovate and address uncertainty.

Resources equipped to address AI and technology changes, as well as changing legal, regulatory and disclosure requirements, are essential in today's volatile environment. As a lack of skilled resources remains a significant risk to organisational success, the committee should evaluate the organisation's skills and capabilities in areas including the following:

Financial planning and analysis (FP&A)

The audit committee should confirm with senior leadership that the organisation's resources have the capability to stress-test financial models across diverse scenarios, including shifting interest rates, currency fluctuations, trade policy shifts and extreme low-probability "black swan" events. Scenario analyses should account for variations in global and national trade policies — tariffs, export controls, subsidy programs — and for fiscal or budgetary changes under new legislation such as the "One Big Beautiful Bill Act."

The audit committee may want to inquire about FP&A's coordination with operating teams to understand the impact on the flow of goods and to update forecasts for supply chain costs, transfer-pricing risks and fiscal policy changes. As part of its oversight role, the committee should understand how FP&A collaborates with risk, legal and tax experts to incorporate legislative developments into forecasts while maintaining documented controls over model adjustments, data inputs and disclosure practises. Comprehensive stress-testing, clear assumptions and strong disclosure controls will help organisations navigate volatility and sustain stakeholder trust.

Accounting and financial reporting

Resources should be allocated to new accounting and disclosure requirements, such as self-developed technology and sustainability reporting — particularly under the European Union's Corporate Sustainability Reporting Directive (CSRD). Disclosures should transparently reflect assumptions, uncertainties and judgment calls embedded in forecasts. The audit committee should ask management to explain key decisions in financial ranges supported by potential outcomes and scenarios, rather than cite a single number, and thereby frame decisions within a spectrum of possibilities, risks and rewards.

The committee also should consider adjustments for geopolitical events and emphasise appropriate governance of non-GAAP metrics and forward-looking estimates. Through a review of filings, committee members should confirm their agreement that management discussion and analysis (MD&A) disclosures on sensitivity analyses and risk mitigation align with investor expectations and evolving Securities and Exchange Commission (SEC) guidance on forward-looking information.

Executive leadership

Storytelling is emerging as a market differentiator. The audit committee should assess the effectiveness of the CEO's and CFO's communications with the investment community. Committee members can strengthen oversight by listening to analyst calls, understanding issues raised, and debriefing with the CEO and CFO. Assigning directors to review competitors' earnings calls can enable comparative analysis, and leveraging AI tools can make this process more efficient and insightful.

Beyond assessing internal skills and capabilities, management must consider the strategic utilisation and mix of third parties — including consulting firms, contractors and offshore resources — to supplement subject matter expertise and address spikes in demand. By focusing on these areas with senior leadership, the audit committee can help ensure organisational resilience and effective governance in a rapidly changing landscape.

Why it matters

In times of volatility, talent is as critical to governance as capital is to growth. Audit committees that understand the organisation's financial, analytical and leadership capabilities can better anticipate risks, evaluate assumptions and challenge management's thinking. Strengthening talent strategy internally and through external partnerships positions the company to respond quickly to uncertainty, maintain transparency and sustain investor confidence.

Key questions to ask

- Does the organisation have a talent strategy aligned with its long-term strategic plan and future objectives?
- Beyond technical skills, how is the organisation cultivating curiosity, ethical reasoning and relationship-building capabilities?
- How is the organisation prioritising areas of focus for additional talent investment?
- Has the organisation gone through an honest evaluation of current capabilities and determined where the strategic use of third parties can close gaps in subject matter expertise?
- How has innovation, including AI application, been incorporated into the talent strategy and resource development program?
- Have changes to workforce composition been sufficiently evaluated for impact on internal control and broader risk management objectives?

6. Align on regulatory risk tolerance.

Regulatory change ranks among the top five enterprise risks globally, along with geopolitical volatility — making clear board alignment on risk appetite and tolerance a governance imperative.[9] In many organisations, the audit committee oversees management's processes for risk identification and assessment, including scenario planning and horizon scanning, and mitigation. In the U.S., an easing of certain federal enforcement priorities — combined with a patchwork of evolving state-level rules over sustainability, data privacy and cybersecurity, as well as CSRD implications for global reporters — demands clarity on how much regulatory risk the company is prepared to accept. Board-level oversight of management's alignment of risk appetite with strategy and disclosures is now a critical stakeholder expectation.

Determining regulatory risk tolerance should be formalised through the ERM framework and the Three Lines Model. Yet maturity gaps persist: Only 30% of organisations report having a centralised, integrated risk management program run by senior management. Board visibility is also uneven — just 64% of boards receive periodic compliance reports, and only 52% have formal compliance oversight — suggesting risk tolerance may not always be consistently understood, defined or operationalised.[10]

Amid ongoing global economic and political volatility, audit committees must remain vigilant in overseeing management's disclosures within financial reporting related to cyber and AI, along with sanctions, tariffs, supply chain disruptions and inflation, particularly in the MD&A and risk factors. The committee should also work with management to implement continuous, risk-based monitoring for regulatory developments across all material jurisdictions and encourage coordinated reporting (where possible) that connects compliance metrics, such as privacy incidents, control effectiveness and regulatory updates, to risk management activities.

[9] *2026 Risk in Focus: Hot topics for internal auditors*, The Institute of Internal Auditors and the Internal Audit Foundation, 2025.

[10] *State of Risk & Compliance Report*, NAVEX Global, 2025.

Why it matters

As regulatory demands intensify, the gap between a company's stated risk appetite and its real exposure can quickly translate into compliance failures or reputational harm. Audit committees that strive to foster a shared understanding of regulatory risk tolerance can bridge the gap by helping leadership balance opportunity with accountability and maintain credibility across markets and jurisdictions.

Key questions to ask

- How are regulatory risk tolerance and compliance posture determined across key areas such as sustainability, data privacy and cybersecurity — and what mechanisms can help ensure they are consistently understood across the organisation?
- Are current governance structures and controls agile enough to respond to rapidly evolving and fragmented global and state-level regulations without exposing the company to undue risk?
- How effective is management reporting at keeping the board adequately informed in a changing environment?

7. Assess culture as a mechanism to drive ethical behaviour.

According to the Anti-Fraud Collaboration's *The Impact of a Changing Work Environment on Corporate Culture*, "A strong ethical culture is a defence against all the conditions identified in the fraud triangle — pressure, opportunity and rationalisation. A robust and positive culture centred on integrity and ethics is key to deterring and detecting fraud."[11]

Boards too often rely on informal and sporadic updates on organisational culture. To strengthen oversight and trust, culture should be a standing board topic, with management presenting structured data and behaviour-based metrics alongside financial and operational risks.[12] While 51% of board directors say they discuss corporate culture during meetings, only 53% of those report having insightful data to assess it.[13]

An organisation's culture is a leading indicator of underlying risk, shaping how employees respond under pressure, rationalise behaviour,

[11] *The Impact of a Changing Work Environment on Corporate Culture*, Anti-Fraud Collaboration, March 2025.

[12] *2025 Organisational Culture and Ethics Report: Tackle Culture Risks in the GRC Ecosystem*, AuditBoard, 2025.

[13] "Three Areas Where Boards Spend Their Time But Don't See Results," Russell Reynolds Associates, Feb. 24, 2025.

and recover from crises both small and large. Ideally, management should monitor culture through surveys, behavioural analytics and incident trends, and not just episodic reviews.[14] Remote and hybrid work heighten the need for culture metrics (e.g., use of anonymous reporting channels, tone in communications) and informal norms assessments to detect early warning signs of rationalisation or opportunity for misconduct.[15]

Continual reassessment of fraud risk is critical as individuals may increasingly justify unethical behaviour. The audit committee should confirm that management's fraud risk assessments account for evolving rationalisation factors — such as economic strain or shifting performance incentives — and that control design (e.g., segregation of duties, automated analytics) adapts accordingly.[16] Collaboration with ERM and internal audit can help ensure culture metrics (e.g., exit interview insight, peer comparison) feed into enterprisewide risk reporting, enabling the committee to challenge management on vulnerabilities and the effectiveness of remedial actions.[17]

The audit committee should also oversee the robustness of whistleblower hotlines, escalation protocols and crisis management plans — whether arising from ethics breaches or other business continuity issues. For instance, crisis teams must have preapproved authority to isolate affected units, engage external advisers and communicate transparently to stakeholders — limiting reputational damage and preserving operational resilience. Routine testing and feedback loops, led or certified by internal audit, can help enhance resilience.[18]

Why it matters

Culture is both a control and a signal. When boards and audit committees treat culture as a measurable, reportable component of risk oversight, they can gain early visibility into behavioural trends that can prevent misconduct before it becomes material. Proactive monitoring of the company's culture, paired with clear accountability for ethics and escalation, helps sustain organisational integrity, reinforce trust and strengthen resilience in times of pressure or change.

Key questions to ask

- Is management's process for monitoring culture as a leading indicator of risk sufficiently robust?
- Are mechanisms in place to inform and enable decisive committee response to reputational crises or egregious ethical breaches?
- In an environment where individuals may increasingly rationalise potentially unethical behaviour, is the committee comfortable that fraud risks are being continuously assessed?

[14] *2025 Organisational Culture and Ethics Report: Tackle Culture Risks in the GRC Ecosystem*, AuditBoard, 2025.

[15] *Tone at the Top*, Issue 130, The IIA, August 2025.

[16] *The Impact of a Changing Work Environment on Corporate Culture*, Anti-Fraud Collaboration, March 2025.

[17] *Tone at the Top*, Issue 130, The IIA, August 2025.

[18] "AI Crisis Preparedness: Key Roles for Boards and Internal Audit," by Mike Levy, NACD, Sept. 12, 2024.

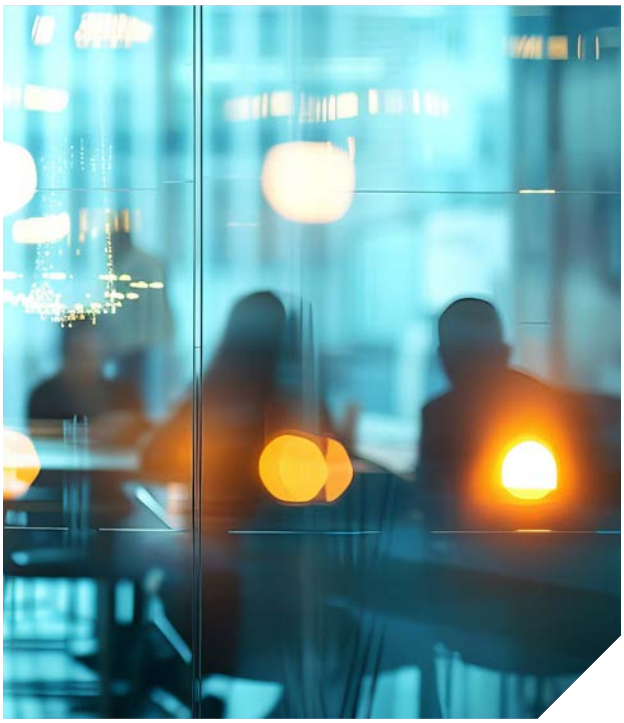
8. Evaluate audit committee expertise and composition as expectations expand beyond financial reporting.

In today's multifaceted risk landscape, the audit committee's role often extends beyond traditional financial oversight. The committee must critically assess its own expertise and composition to ensure effective monitoring and interpretation of emerging risks related to AI implementation, cybersecurity, ethics, sustainability and other nonfinancial areas. This evaluation requires a coordinated approach with the full board to allocate oversight responsibilities clearly and periodically review and update them as they evolve. If the committee's responsibilities are expanding, its composition and skill sets must evolve accordingly.

The audit committee should identify and prioritise acting on the gaps through training, recruiting new directors or engaging external advisers. A key focus is ensuring the committee possesses a balanced mix of skills aligned with its charter, potentially including cyber risk management; data privacy; environmental, social and governance (ESG); AI governance; technology; ethics; and ERM. Continuous education and director development are essential to stay current with regulatory changes and emerging risk trends, ensuring that every committee member can contribute meaningfully to strategic oversight.

Regular self-assessment is also critical. The committee should periodically evaluate its performance and expertise, focusing on meeting effectiveness, skill depth and opportunities for improvement. As AI adoption broadens the scope of available analysis, committees will increasingly pair retrospective reviews of historical data with forward-looking tools for predictive and trend analysis. This will enable the committee to be more proactive and informed in collaborating with management.

The committee's skills and performance may be challenged to keep pace.[19] Ultimately, audit committee composition should be aligned with the complexity of the change environment the organisation faces.



[19] "The Artificially Intelligent Boardroom," by David F. Larcker, Amit Seru, Brian Tayan and Laurie Yoler, *Stanford Closer Look Series*, Corporate Governance Research Initiative, Stanford Graduate School of Business, March 2025.

Why it matters

As audit committee mandates expand, expertise must keep pace. Boards that continuously review committee composition and invest in director development build the agility to oversee fast-moving, technology-driven risks. Regular self-assessment and upskilling strengthen oversight, accountability and the committee's readiness for what's next.

Key questions to ask

- As the committee's role evolves, is management providing the right level of integrated assurance across financial, operational, technology and strategic risks aligned with the committee's chartered mandate? Are reporting mechanisms fit for purpose?
- Are annual reviews conducted of risk management systems, policies and procedures, with presentations on leading practises tailored to the company's industry and regulatory environment?
- When was the last time the committee completed a self-assessment of its performance, including an analysis of current skills required to deliver on all aspects of its governance responsibilities?

9. Understand and support internal audit's reinvention for the future.

The audit committee should seek to understand the CAE's vision for the future of the internal audit function by reviewing the function's strategic plan and validating that the CAE is taking proactive steps to stay current with — or ahead of — emerging trends. The committee can leverage tools such as the refreshed *Next Generation Internal Audit Framework*[20] to guide discussions on how internal audit will:

- Align clearly with enterprise priorities and stakeholder needs
- Deliver technology-enabled insights that drive smarter, more informed decisions
- Operate with agility and adapt to emerging risks and rapid change
- Collaborate effectively across assurance and advisory functions for broader impact
- Operate strategically and in accordance with The IIA's Global Internal Audit Standards

[20] *The Next Phase: AI and Human Collaboration Powering Internal Audit Transformation*, page 6, Protiviti, June 2025.

The rapid evolution of generative AI is reshaping how audits are conducted, shifting internal audit from sample-based, manual testing to continuous, autonomous assurance and real-time insights. This transformation promises greater efficiency, coverage and strategic relevance. However, it also raises questions about preserving the human element in auditing. Many organisations already use generative AI to summarise data and produce reports, yet the emerging wave of agentic AI — capable of performing end-to-end testing, risk sensing and anomaly detection — demands new skill sets and guardrails.[21]

A human-in-the-loop approach remains essential. While AI can handle repeatable tasks and analyse vast datasets, only auditors can bring the contextual judgment, empathy and situational awareness needed for nuanced decision-making and stakeholder engagement.[22] The question is not just how AI will replace manual tasks, but also how it can augment human expertise, blending algorithmic speed with professional discernment and humanistic qualities. Internal audit must both sensibly integrate AI within its own practises and play a critical role in evaluating the organisation's overall governance of AI adoption.

Why it matters

The accelerating integration of AI into assurance activities places new demands on internal audit. Success will depend on the function's capacity to combine advanced technology with professional skepticism, ethical judgment and business acumen. Through active oversight and partnership, audit committees can help ensure internal audit remains a trusted, independent adviser that strengthens governance, enhances transparency and upholds confidence in the company's integrity.

Key questions to ask

- In what areas of the internal audit process are AI approaches being explored, and how are they being applied?
- As the internal audit function embeds AI into its workflows, is the importance of critical thinking, empathy and practicality being stressed in talent and training strategies?
- How does internal audit's strategy leverage technology and incorporate the development or acquisition of talent to achieve its strategic objectives?
- How is internal audit leading coordinated coverage with other assurance functions such as risk, controls and compliance?

[21] *2026 Risk in Focus: Hot topics for internal auditors*, The Institute of Internal Auditors and the Internal Audit Foundation, 2025.

[22] *Tone at the Top*, Issue 129, The IIA, June 2025.

About the authors

ANDREW STRUTHERS-KENNEDY
Protiviti Managing Director
Global Leader, Internal Audit and Financial Advisory & CAE Solutions

As the global lead of Protiviti's Internal Audit and Financial Advisory practise, 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, CAE Solutions

Gordon Braun is in Protiviti's Internal Audit and Financial Advisory practise 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 practise and has nearly three decades of experience. Kristen is deeply 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 practises, Sarbanes-Oxley compliance and risk management.

Acknowledgements

We wish to thank Protiviti subject matter experts Jim DeLoach, Chris Wright, Charlie Soranno and Ari Sagett for their contributions to this publication.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 10th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

11,000+	90+	25+	$2 BN
Protiviti professionals*	office locations worldwide	countries	in revenue*

The Americas

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

Europe, Middle East & Africa

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA*
Durban
Johannesburg

Asia-Pacific

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®