



2026 Nordic Internal Audit Survey

A Nordic perspective on the evolving Internal Audit landscape

June 2026

Introduction



This report presents the first edition of the KPMG Nordic Internal Audit Survey, and we thank all Internal Audit leaders who participated.

The survey is based on responses from **Internal Audit leaders across the Nordic region**, representing a broad range of industries and organization sizes. More than 70% of respondents represent organizations with over 1,000 employees, including large multinational enterprises.

The purpose of the survey is to provide practical insights into key priorities, challenges, and emerging practices shaping Internal Audit functions. It reflects how functions are responding to an evolving risk and technology landscape, particularly cybersecurity and artificial intelligence.

The findings show growing interest in AI-enabled auditing and digital capabilities, with **around 75% of Internal Audit functions already using or planning to use AI tools**. At the same time, maturity across strategy, governance, data, and skills remains uneven.

This gap between rising expectations and constrained capacity highlights the need for stronger competencies and foundational enablers as Internal Audit roles continue to expand.

We hope these insights support Internal Audit leaders in navigating current challenges and strengthening their role as trusted advisors.

Survey at a glance

- 47 Internal Audit leaders participated
- Coverage across 5 Nordic countries
- >70% of respondents represent organizations with over 1,000 employees

Table of contents and key findings:

1. Cybersecurity and AI Are Reshaping the Internal Audit Agenda

- Cybersecurity and AI have become central drivers of Internal Audit priorities, reshaping assurance focus and stakeholder expectations.
- What should Internal Audit evolve its role to remain relevant as cyber risk and AI become enterprise-critical?

[More on page 04 →](#)

2. AI Strategy and Adoption in Internal Audit: Progress, but Uneven Maturity

- While AI strategies are increasing, Internal Audit functions show variation in readiness and ability to scale adoption.
- How many of these strategies remain as an open question?

[More on page 07 →](#)

3. Data Quality and Access Constrain Advanced Assurance

- Limitations in data quality and access provision, continue to restrict the effectiveness of AI-enabled and data-driven assurance.
- What must change in data foundations for IA to fully leverage analytics and AI?

[More on page 10 →](#)

4. Skills and Competencies Are a Critical Enabler of Future Internal Audit

- Gaps in digital and AI-related skills are emerging as one of the most significant barriers to advancing Internal Audit capabilities.
- What skills do internal auditors need, to effectively operate in a technology-driven risk landscape?

[More on page 13 →](#)

5. AI Governance, Ethics and Transparency Drive Risk Concerns

- Concerns around AI governance, ethics, and transparency, are increasing expectations on providing informed and credible assurance.
- How can Internal Audit provide assurance over emerging technologies while risks and regulations continue to evolve?

[More on page 16 →](#)





1. Cybersecurity and AI Are Reshaping the Internal Audit Agenda

Internal Audit must shift from coverage and efficiency toward deeper, technology-driven assurance to remain relevant

Keeping Internal Audit relevant as technologies evolve

The survey illustrates a clear transition for Internal Audit: from established coverage of cybersecurity toward increasing expectations around AI and emerging technologies. Although current activity suggests progress, the forward-looking view reveals rising demands that may outpace existing capabilities if not addressed.

Current status



62% of respondents said they are **somewhat prepared** to audit Emerging Technologies.



66% of respondents are planning to auditing Cybersecurity.



38% of respondents are currently auditing AI / Machine learning.



87% of respondents are currently using any form of AI (e.g., Copilot, AI assistant, own developed AI tool) in their Internal Audit activities.

Looking forward

68% of respondents expect Internal Audit to play an **important complementary** role in providing assurance over AI within the next three years, while **15%** expect the role to be **crucial**.

Top 3 emerging audit areas that is expected to require the most attention in the future:

- Cybersecurity and data privacy (87%)
- Third-party and supply chain risks (68%)
- Artificial intelligence (62%)

Top 3 challenges/concerns when auditing AI and Cybersecurity:

AI	01	Lack of technical expertise
	02	Assessing data quality and bias
	03	Technical complexity
Cybersecurity	01	Rapidly evolving threats and vulnerabilities
	02	Lack of technical expertise
	03	Reliance on third parties and vendors

KPMG Insights

While cybersecurity coverage is well established and AI is increasingly used within audit activities, stakeholder expectations are shifting faster than current assurance capabilities. As cyber risk and AI become embedded in core business processes, Internal Audit faces a growing need to evolve its role from established assurance practices toward deeper, more forward-looking oversight of technology-driven risk.

Expectations are outpacing today's readiness

Looking ahead, most respondents expect Internal Audit to play an important or crucial role in providing assurance over AI within the next three years.

However, current preparedness levels suggest that many functions are not yet positioned to meet these expectations as cyber risk and AI become enterprise-critical.

What this means for Internal Audit: *to remain relevant, Internal Audit must reposition itself as a forward-looking assurance partner, aligned with evolving technology risks and stakeholder expectations.*

66% of organizations plan cybersecurity audits, versus 40% for AI

AI is already used internally, but assurance capabilities lag adoption

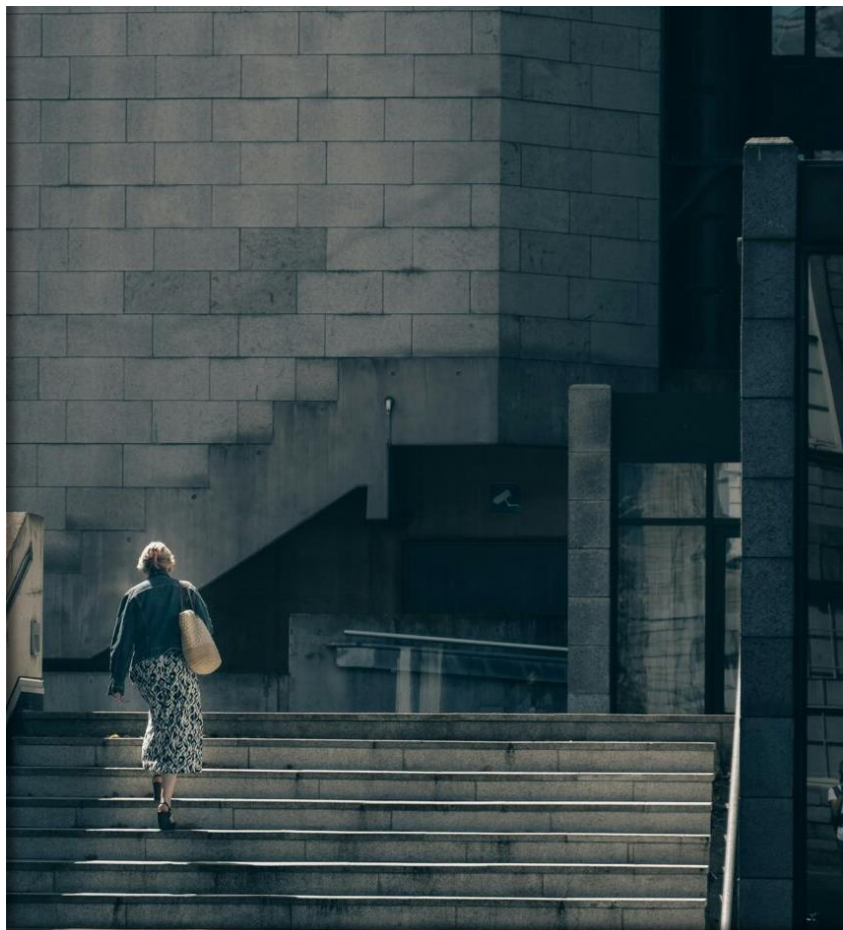
Across the survey, Internal Audit functions report increasing use of AI to support planning, reporting, and analytics, yet far fewer are providing assurance over AI itself. This imbalance indicates that Internal Audit is adopting AI faster than it is assessing AI risk—creating a potential credibility gap as AI becomes more central to business decision-making.

What this means for Internal Audit: *Internal Audit must evolve from using AI primarily as a productivity enabler to independently assessing AI governance, controls, and outcomes.*

Capability gaps are built into the operating model

Survey responses show that when Internal Audit lacks technology expertise, the primary response is to rely on co-sourcing or ad-hoc external support. At the same time, many functions report having no formal strategy or roadmap for auditing AI or emerging technologies pointing to a structural challenge rather than isolated skill shortages.

What this means for Internal Audit: *Internal Audit must move from reactive sourcing toward intentional capability-building through clearer operating models and long-term planning.*





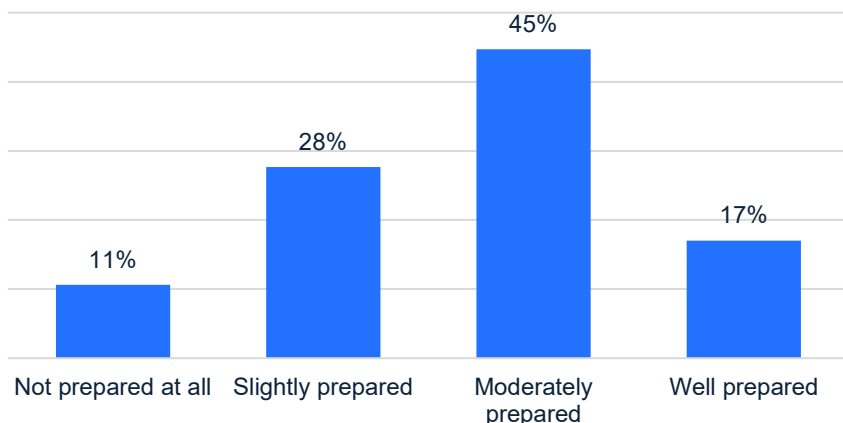
2. AI Strategy and Adoption in Internal Audit: Progress, but Uneven Maturity

Internal Audit has agreed on the strategic importance of AI, but readiness remains limited

AI Strategy and Adoption in Internal Audit: Progress, but Uneven Maturity

While AI strategies are increasing, Internal Audit functions show variation in readiness and ability to scale adoption.

Figure 1: How well prepared is your Internal Audit function to audit the discussed areas (emerging technologies)?



Moderate readiness to audit emerging technologies

Nearly half of respondents assess themselves as only *moderately prepared*, with a small minority indicating high readiness. Suggesting a growing awareness but limited capability to deliver consistent assurance over emerging technologies.

Co-sourcing is the preferred response to skills gaps

When expertise is lacking, Internal Audit primarily co-sources with external specialists rather than fully outsourcing. This reflects a desire to retain ownership, while underscoring ongoing dependency on external capabilities.

AI strategy remains largely aspirational

AI strategies are emerging, but maturity remains uneven. Many Internal Audit functions are still in discussion or early development, indicating a gap between ambition and operational execution.

Figure 2: If you were to audit an area where your organization lacks in-house expertise, how would you proceed?

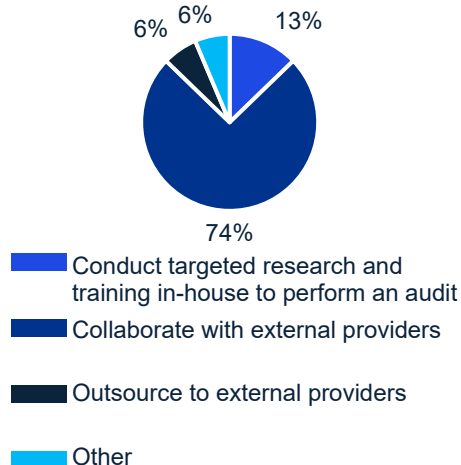
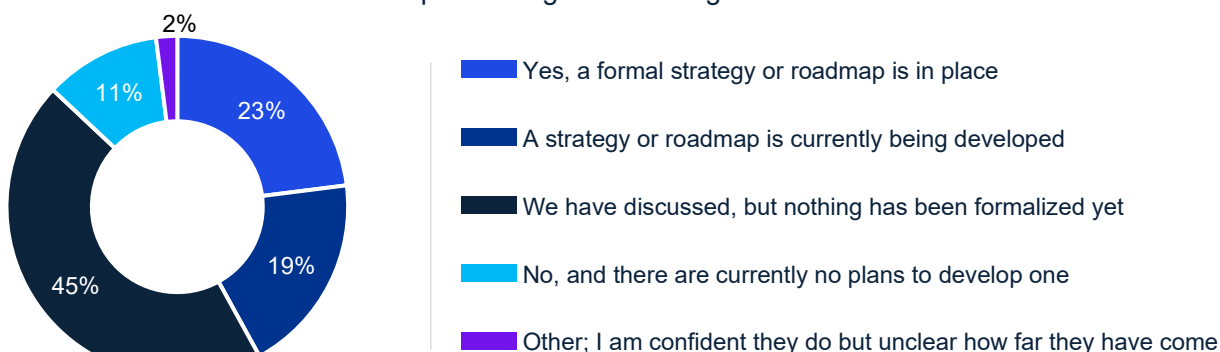


Figure 3: Does your internal audit function have a strategy or roadmap for evaluating and implementing AI technologies?



KPMG Insights

While ambition and awareness are widespread, readiness, clarity of direction, and the ability to scale adoption vary significantly across organizations. Differences in size, sector, and operating complexity continue to shape how effectively Internal Audit can move from strategy to execution, raising important questions about future relevance, capability, and assurance depth in an AI-enabled organization.

Strategy Exists, but the Direction Is Still Unclear

For many Internal Audit functions, AI strategy exists but remains unresolved. AI is acknowledged within organizations as important, yet key questions such as *what exactly should Internal Audit assure? Where should AI be applied first? How much reliance on external expertise is acceptable?* remain open.

Revealing while AI might be present at a strategy level, often lacks finality. Instead of acting as a clear roadmap, it functions as a placeholder, signaling intent without yet defining boundaries, priorities, or ownership. As a result, AI initiatives risk stalling at the discussion stage, unable to progress into structured audit practices.

What this means for Internal Audit: Without clear strategic choices, AI remains a concept rather than a capability, limiting Internal Audit's ability to provide credible assurance in an AI-enabled organization.



From Momentum to Reality: Strategy Is Moving Faster Than Readiness

AI is on Internal Audit's agenda, but confidence in readiness remains low. Only **17% of respondents identify their function as well prepared**, while the majority place themselves in the middle of the maturity spectrum. Suggesting that, despite widespread ambition, most functions recognize a gap between intent and their current ability to deliver consistently.

Larger Internal Audit functions, often embedded in regulated sectors such as financial services or telecommunications, are better positioned to absorb the complexity of AI adoption, but still face scale-related constraints such as governance, coordination, and assurance consistency.

What this means for Internal Audit:

Progress on AI depends less on awareness and more on how ready Internal Audit is in practice. Structure, complexity, and the operating model determine how quickly ambition turns into real assurance.

The Shift from "Should We?" to "How Far Will We Go?"

Organizations agree that Internal Audit should engage with AI, but the real question now is how far organizations are prepared to go. Only 23% of respondents have a formal AI strategy or roadmap in place, with another 19% developing one, while **45% still report that AI strategy remains discussed** but not formalized.

This divide closely reflects differences in size and maturity. Larger Internal Audit functions, often operating across multiple geographies are more likely to move beyond discussion and embed AI into core assurance. Smaller functions tend to adopt a more cautious approach, using AI selectively rather than redefining their assurance role.

What this means for Internal Audit:

The strategic challenge is no longer whether to engage with AI, but how deliberately Internal Audit defines the depth and ambition of its role in an AI-enabled organization.



3. Data Quality and Access Constrain Advanced, AI-enabled Assurance

Limited data quality, access and tooling maturity continue to constrain the effectiveness and scalability of data- and AI-driven Internal Audit

Data Quality and Access Constrain Advanced, AI-enabled Assurance

Limitations in data quality and access provision, continue to restrict the effectiveness of AI-enabled and data-driven assurance. What must change in data foundations for IA to fully leverage analytics and AI?

55% of organizations rely on Excel or Google Sheets instead of a GRC platform, indicating low process and data maturity for risk, controls, and assurance.

83% use Excel or Power Query and 62% use Power BI for audit analytic, highlighting heavy reliance on stand-alone, analyst-driven tools rather than embedded, scalable solutions.

While 58% use data analytics *always or quite often*, usage remains inconsistent and largely manual.

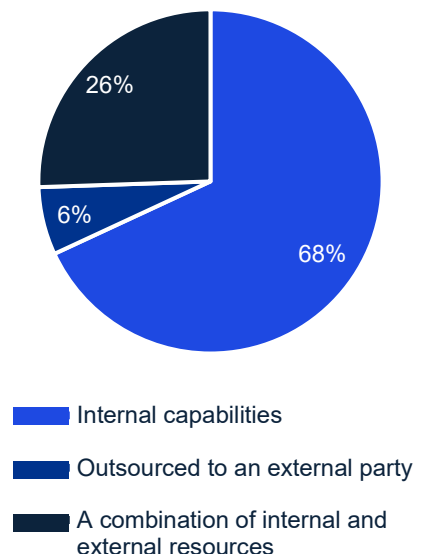
What are the key barriers using AI in internal auditing in your organization?

1. Data access or data quality issues

2. Lack of in-house expertise

3. Technical limitations

Figure 4: How do you conduct data analytics audits?



KPMG Insights

Internal Audit is actively using data analytics and exploring AI, but the step change to advanced, AI-enabled assurance remains constrained by the same foundations. Fragmented data, spreadsheet-driven evidence, and inconsistent access mean that analytics and AI cannot be applied systematically or at scale, limiting their impact on assurance quality and efficiency.

AI readiness is uneven because platform maturity is uneven

The foundation gap creates a “two-speed” reality: smaller/mid-size organizations are far more likely to lack platforming, with Excel/Sheets reliance at 86% (5,001–10,000 employees) and 75% (0–100 and 101–1,000), versus 25% in the largest organizations (10,001+). That uneven baseline directly shapes how far IA can industrialize analytics and AI, because the data foundation determines repeatability, governance, and scale.

What must change: *define and implement a minimum “AI-ready IA data foundation” (standard evidence taxonomy, controlled audit data layer/share, repeatable access provisioning) so IA can leverage analytics and AI consistently regardless of organization size.*



Spreadsheet-first foundations keep IA in “manual mode”

Many teams are still building assurance on spreadsheets rather than a governed system of record, 55% report having no GRC platform and relying on Excel/Sheets, which makes risk/control data fragmented and inconsistent before analytics or AI even starts.

This is most acute in smaller IA teams: 80% of functions with 1–3 internal auditors rely on Excel/Sheets, versus ~30–33% among larger teams.

What must change: *standardize the control universe and evidence metadata in a governed repository (clear control IDs, ownership, frequency, systems, populations, exceptions) so analytics/AI can run on a consistent baseline, not ad-hoc files.*

Even with capability, data access and quality remain the gating factor

Most respondents say they can execute analytics internally (68% internal; 26% hybrid; 6% outsourced), yet AI adoption still stalls at the same point: data access or data quality issues (60%) is the top barrier, ahead of lack of in-house expertise (38%) and technical limitations (34%). This barrier persists regardless of delivery model (reported by 75% of fully in-house and 70% of co-sourced models), pointing to a structural constraint rather than a skills-only gap.

What must change: *establish an audit-ready data access model (role-based access, pre-approved datasets, controlled environments) and a data stewardship routine that prioritizes audit-critical data elements, so access and quality become predictable, not negotiated each engagement.*





4. Skills and Competencies Are a Critical Enabler of Future Internal Audit

The future of Internal Audit will be defined less by technical specialization, and more by hybrid skills that connect technology, data, and governance

Skills and Competencies Are a Critical Enabler of Future Internal Audit

Barriers to Advance in Internal Audit Capabilities

Skills gaps dominate across emerging tech topics; data quality and rapid change are the next most common constraints.

Internal Audit Area	Main challenge / concern
AI	Lack of technical expertise
IT / Cloud Computing	Lack of technical expertise
Cybersecurity	Rapidly evolving threats and vulnerabilities
Data Analytics	Challenges in data integration and quality
Automation (RPA)	Complexity in integrating automation with existing systems
Internet of Things	Lack of technical expertise
ESG	Data quality, availability, and reliability
Finance & Accounting	Inconsistent or undocumented business processes

62% of Internal Audit teams have received AI-related training relevant to audit work, 38% have not

Future Skills and Competencies in Internal Audit

To operate effectively in an increasingly technology-driven risk landscape, Internal Audit must strengthen capabilities beyond traditional audit skills. Data literacy, AI understanding, and technology risk knowledge are becoming core audit competencies rather than specialist add-ons.

In practice, this skills gap is currently bridged through collaboration, as evidenced by the fact that 57% of organizations rely on external consultants or other departments for AI-related initiatives, highlighting both progress and continued dependency.

Which emerging technologies has your Internal Audit team developed or is developing expertise in auditing?

1. Artificial Intelligence
2. Robotic Process Automation
3. Cloud Computing

Which emerging technologies does your Internal Audit team intend to focus on for developing audit methodologies in the next 12 months?

1. Artificial Intelligence
2. Machine Learning
3. Robotic Process Automation
4. Cloud Computing

KPMG Insights

Internal Audit is actively exploring AI and other emerging technologies, but progress is constrained by uneven skill development and foundational gaps. While AI has clearly become a priority, training, supporting technical competencies, and preparedness vary significantly across teams and markets. As technology-driven risks increasingly cut across data, systems, and business processes, these capability gaps are shaping how effectively Internal Audit can deliver scalable, consistent, and credible assurance.



AI is the center of gravity, but the skills around it remain shallow

Internal Audit has clearly aligned around AI: roughly three-quarters of teams report existing or developing expertise in AI, and a similar proportion plan to focus future methodology development there. Yet this focus is not matched by comparable investment in cloud, automation, and data analytics, which lag far behind. As a result, many teams are preparing to audit AI without fully strengthening the technical foundations that AI depends on.

What this means for Internal Audit: the demand signal for AI assurance is loud, but capability is still narrow. Auditing AI credibly requires broader supporting skills, particularly in data, cloud environments, and automated controls, not AI awareness alone.

Training is the clearest make-or-break gap, and it is unevenly distributed

On the surface, progress is visible: around 60% of Internal Audit teams report having received AI-related training relevant to audit work. But this masks a structural divide. Nearly 4 in 10 teams either lack training entirely or are only planning to start, leaving real capability fragmented. The gap widens further for smaller audit teams and across markets, where access to training, time, and funding differ materially.

What this means for Internal Audit: AI readiness is less about intent and more about enablement. Without deliberate investment in training, many audit functions will struggle to move beyond ad-hoc reliance toward scalable AI assurance.



The future Internal Auditor is hybrid, not a technical specialist

The findings point to a shift in the auditor profile. As emerging technologies proliferate, most teams are not building deep expertise across every domain. Instead, capability is concentrating where risk pressure is highest, with AI far ahead of other technologies. In this environment, value comes from technical fluency combined with audit judgment, rather than specialist depth. The ability to challenge governance, question data flows, and interpret risk across systems becomes more critical than mastering individual tools.

What this means for Internal Audit: long-term relevance will depend on hybrid skill sets that connect technology, process, and governance, enabling Internal Audit to provide insight and assurance without needing to be experts in everything.





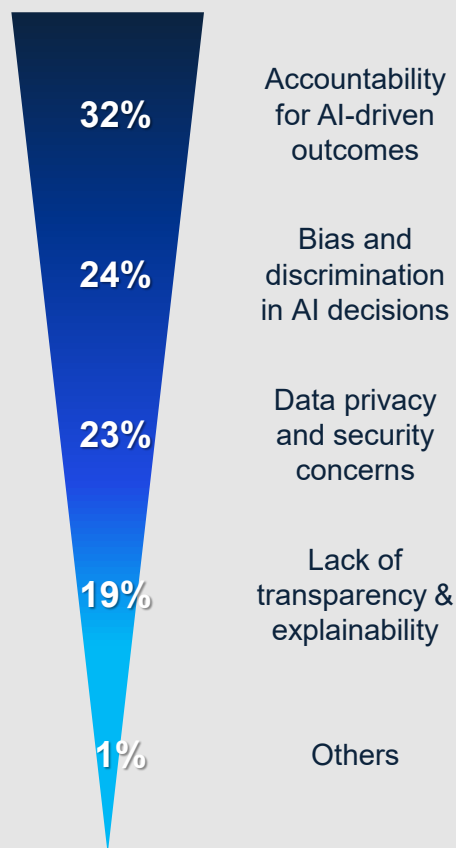
5. AI Governance, Ethics and Transparency Drive Risk Concerns

As AI scales, expectations shift from knowing the risks to proving who owns and controls the outcomes

AI Governance, Ethics and Transparency Are the Primary Risk Drivers

Concerns around AI governance, ethics, and transparency, are increasing expectations on providing informed and credible assurance. How can Internal Audit provide assurance over emerging technologies while risks and regulations continue to evolve?

Figure 5: Main risks or ethical challenges associated with AI from an audit perspective:

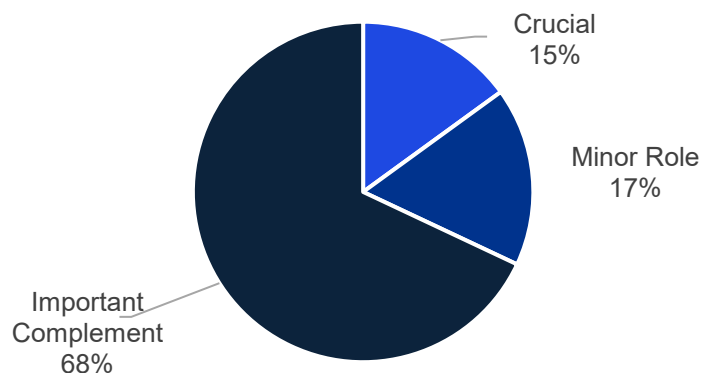


As AI becomes more embedded in business decisions, **accountability** for AI-driven outcomes emerges as the **leading ethical concern**.

Risks related to bias and discrimination, and data privacy and security, follow closely, reflecting **persistent challenges around fairness and data protection**.

Transparency and explainability remain important in shaping confidence in AI outcomes, reinforcing a **focus on governance, control, and trust**.

Figure 6: What role do you expect Internal Audit to play in providing assurance over AI within the next 3 years?



As organizations look ahead, Internal Audit is most commonly expected to play an important **complementary role in providing assurance over AI (68%)**, rather than acting as the primary owner.

A smaller share view Internal Audit as having a crucial role (15%), while others see its involvement as more limited (17%). This suggests an evolving position for Internal Audit, supporting AI assurance while accountability remains shared across the organization.

What this means for Internal Audit?

As concerns around AI accountability, bias, and transparency intensify, expectations on Internal Audit to provide credible assurance over AI governance are rising.

IA is increasingly expected to assess whether governance, controls, and oversight are fit for purpose, while acting as a key assurance partner, not the sole owner of AI risk. To remain relevant, Internal Audit must evolve its approach, with a stronger focus on governance, transparency, and control effectiveness as AI risks, technologies, and regulatory expectations continue to develop.

AI Governance, Ethics and Transparency Are the Primary Risk Drivers

Concerns around AI governance, ethics, and transparency, are increasing expectations on providing informed and credible assurance. How can Internal Audit provide assurance over emerging technologies while risks and regulations continue to evolve?

Internal Audit is expected to validate governance, not own AI risk	Nearly 70% of respondents expect Internal Audit to play an important complement role in AI assurance, while only 15% expect a crucial role. This indicates strong expectations on assurance and oversight, while risk ownership remains with the business. This reinforces that accountability for AI outcomes remains distributed across the organization. Internal Audit's value lies in independently validating that governance, transparency, and oversight mechanisms work in practice, not assuming responsibility for managing AI risk. What must change: Internal Audit must clearly anchor its mandate around governance effectiveness and oversight validation, reinforcing independence from risk ownership.
--	---

AI maturity shifts assurance from understanding risk to evidencing control	Even among organizations already using AI, there are growing expectations for credible, evidence-based assurance. As AI moves into real workflows, stakeholders shift focus toward proof that risks such as accountability (74%), bias (55%), and data privacy (53%) are actively monitored and controlled, not just recognized. What must change: Internal Audit must evolve from awareness-driven reviews to outcome-focused assurance, demonstrating that AI risks remain controlled as AI use scales, while maintaining a clear second-line challenge role.
--	--



Accountability is becoming the defining AI risk

As AI moves from pilots into core business decisions, accountability for AI-driven outcomes has emerged as the dominant concern. The question organizations are now asking is no longer whether AI works, but who owns the outcome when it fails, misleads, or causes harm.

This shift is driving higher expectations on Internal Audit to provide assurance that accountability is clearly assigned, embedded in governance, and supported by operational controls, without taking on the ownership of those decisions.

What must change: Internal Audit must move beyond framework validation and focus assurance on decision ownership, escalation paths, and outcome accountability across the AI lifecycle, while preserving its independent assurance role.



kpmg.se | kpmg.no | kpmg.fi | kpmg.dk | kpmg.is



Oksana Muzychenko

Sweden

E: oksana.muzychenko@kpmg.se



Frank Sundgaard Nielsen

Denmark

E: fsnielsen@kpmg.com



Kenneth Hansen

Norway

E: kenneth.hansen@kpmg.no



Christian Liljeström

Finland

E: christian.liljestrom@kpmg.fi



Gunnar Ragnarsson

Iceland

E: gragnarsson@kpmg.is

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG AB, a Swedish limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.