2026 Internal audit priorities annual survey



Jefferson Wells®

NOW PART OF SIKICH®

Table of contents

Executive summary 03

Internal audit priorities 04

Cybersecurity and technology risk 10

Internal audit growth 15

Talent 20

Artificial intelligence 25

Conclusions 32

Executive summary

Internal audit's priorities may look familiar, but the environment surrounding them has become more demanding. Cybersecurity and artificial intelligence (AI) remain dominant risks, while economic uncertainty, regulatory requirements and technology transformation add complexity across the organization.

The larger story in 2026 is the continued expansion of internal audit's mandate. Audit functions are expected to address a broader range of risks and provide deeper assurance in rapidly evolving areas. While budgets and hiring are increasing, many Chief Audit Executives still report gaps in time, resources, and specialized expertise.

Technology is also reshaping the internal audit operating model. Internal audit leaders now compete with the broader technology sector for cyber, AI, and data skills. As a result, many functions are combining internal organizational knowledge and auditor judgment with specialized external support.

Meanwhile, AI is becoming embedded in audit planning, fieldwork, testing, and reporting, while internal audit is increasingly responsible for assurance over its expanding organizational use. This dual role creates an important tension: internal audit is increasingly assessing whether AI is governed securely, but focusing less on whether models are accurate, effective, and operating as intended. The findings that follow can help internal audit leaders benchmark their functions, uncover potential blind spots, and focus resources where stronger capabilities and assurance are needed most.

Internal audit priorities

Cybersecurity and AI remain top priorities, while immediate operating pressures divert focus from long-term strategy.

Familiar priorities, a faster-moving risk environment

The priorities are familiar. The speed, complexity and interdependence of the risks are not.

Cybersecurity and artificial intelligence remain the defining risks for internal audit leaders in 2026. Their continued prominence does not mean the risk environment has stabilized. The technologies, threats, regulations, and organizational dependencies within these categories continue to evolve, requiring audit functions to continually revisit their understanding and coverage.

Meanwhile, economic uncertainty and regulatory change are drawing attention to immediate business pressures. Strategic risk has declined in this year's rankings, suggesting that internal audit leaders are allocating more of their limited capacity to risks with near-term operational consequences.

Comparing internal audit leaders and audit committees adds another dimension to the story. Both groups remain broadly aligned on cybersecurity, AI, and regulatory compliance. However, Chief Audit Executives focus more on shorter-term uncertainty, while audit committees focus more on strategy, resilience, and privacy.

This distinction does not necessarily represent misalignment. It highlights the different time horizons each group brings to risk oversight. Internal audit can create value by connecting immediate assurance activity to the committee’s longer-term view of organizational resilience and strategy.

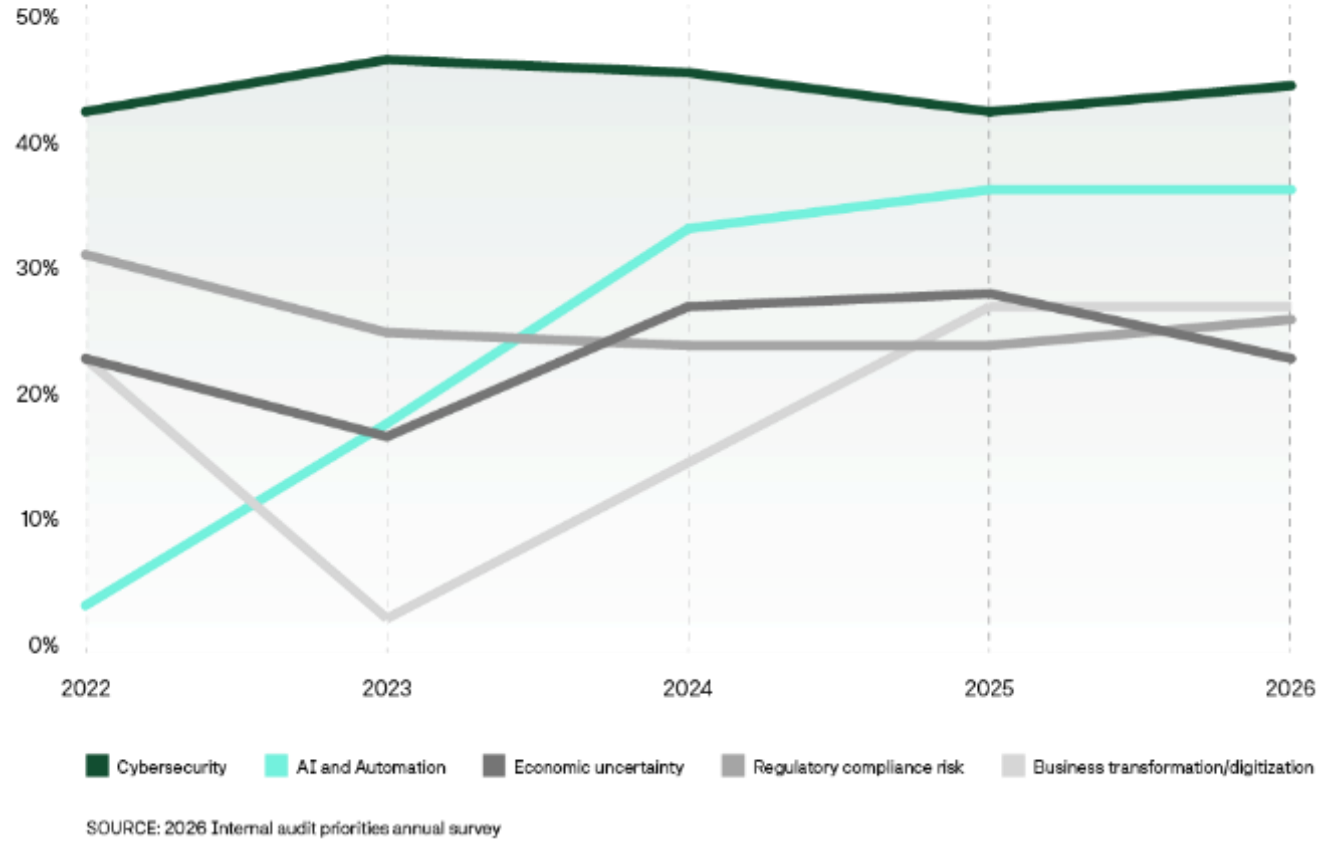
Cybersecurity and AI continue to dominate

Among the internal audit leaders surveyed, cybersecurity has remained the most frequently selected emerging risk over the past five years. It rose slightly from 41% in 2025 to 43% in 2026, while AI and automation held steady at 35% after climbing rapidly from just 3% in 2022.

The year-over-year results also show greater attention to disruption and uncertainty risks. Regulatory compliance increased from 23% to 25%, while economic uncertainty remained elevated at 26%.

Together, these trends suggest that internal audit leaders are concentrating on risks that are evolving quickly or creating more immediate operational consequences. Cybersecurity and AI continue to anchor the risk agenda, but the surrounding priorities reflect pressure to respond to a changing regulatory, economic, and technology environment.

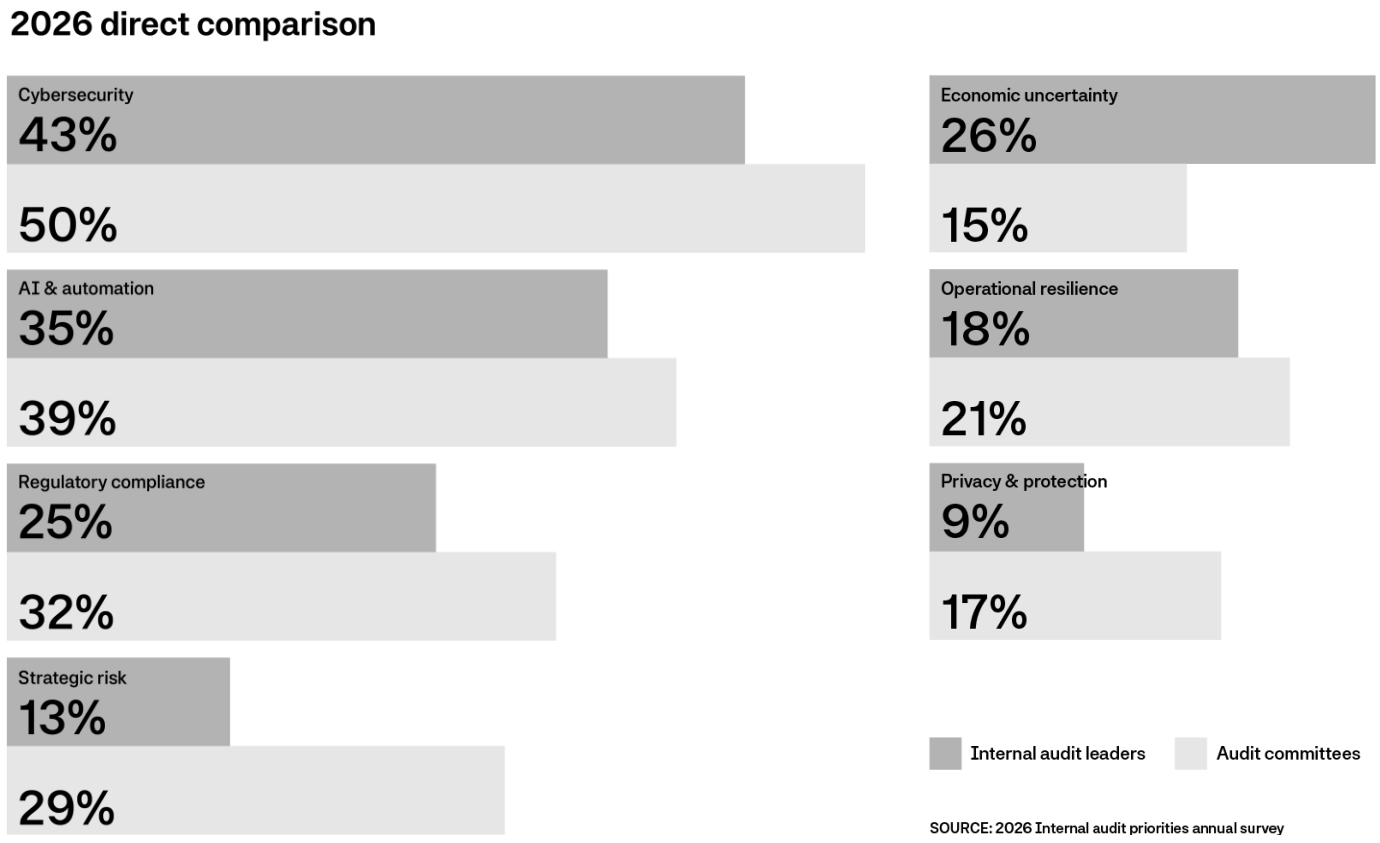
Five-year trend in internal audit leaders' top emerging risks



SOURCE: 2026 Internal audit priorities annual survey

Internal audit leaders and audit committees operate on different horizons

This is the first year the results have been this closely aligned. Both groups align on cyber, AI, and regulatory compliance. CAEs focus more on shorter-term uncertainty, while committees emphasize longer-term strategy, resilience, and privacy.



SOURCE: 2026 Internal audit priorities annual survey

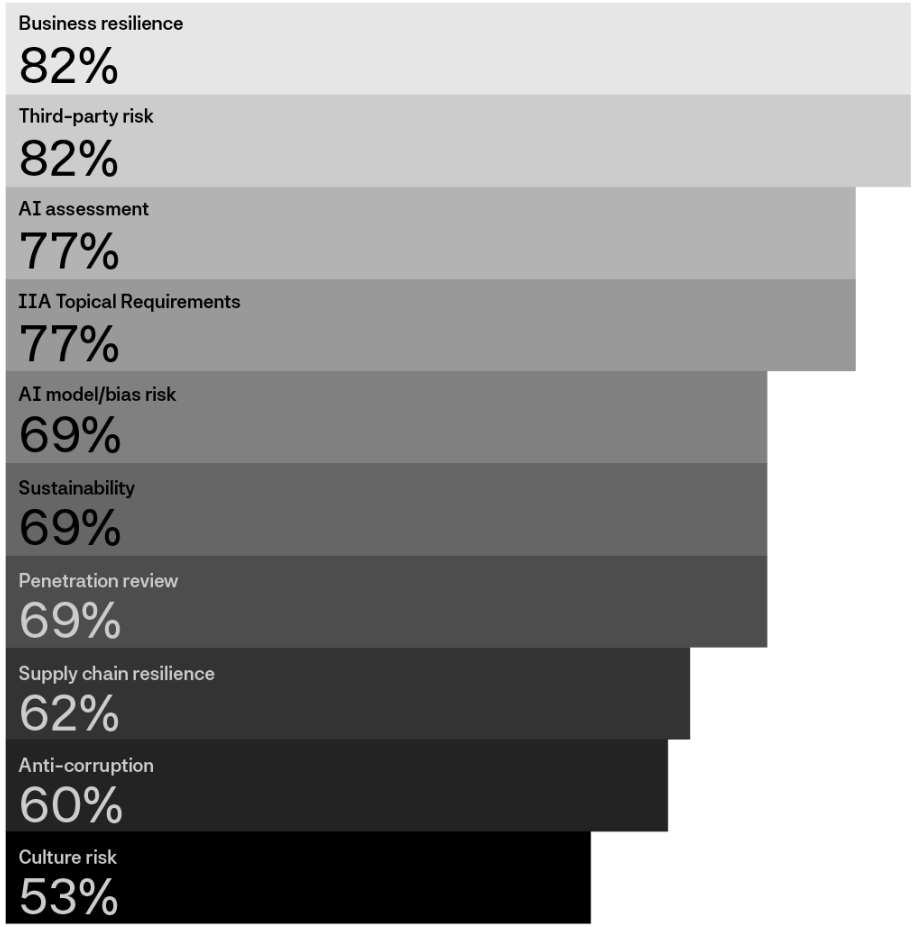
Audit plans are broad, but important gaps remain

More than 80% of audit plans include business resilience and third-party risk, while 77% include both AI assessments and audits addressing applicable IIA Topical Requirements.

However, nearly 25% do not include AI or Topical Requirements, and 38% do not include supply chain resilience. While not exhaustive, these results highlight emerging and important topics whose inclusion in audit plans has historically been inconsistent.

The challenge is not identifying more risk. It is providing sufficient assurance across the expanding risk universe.

Areas currently included in the audit plan

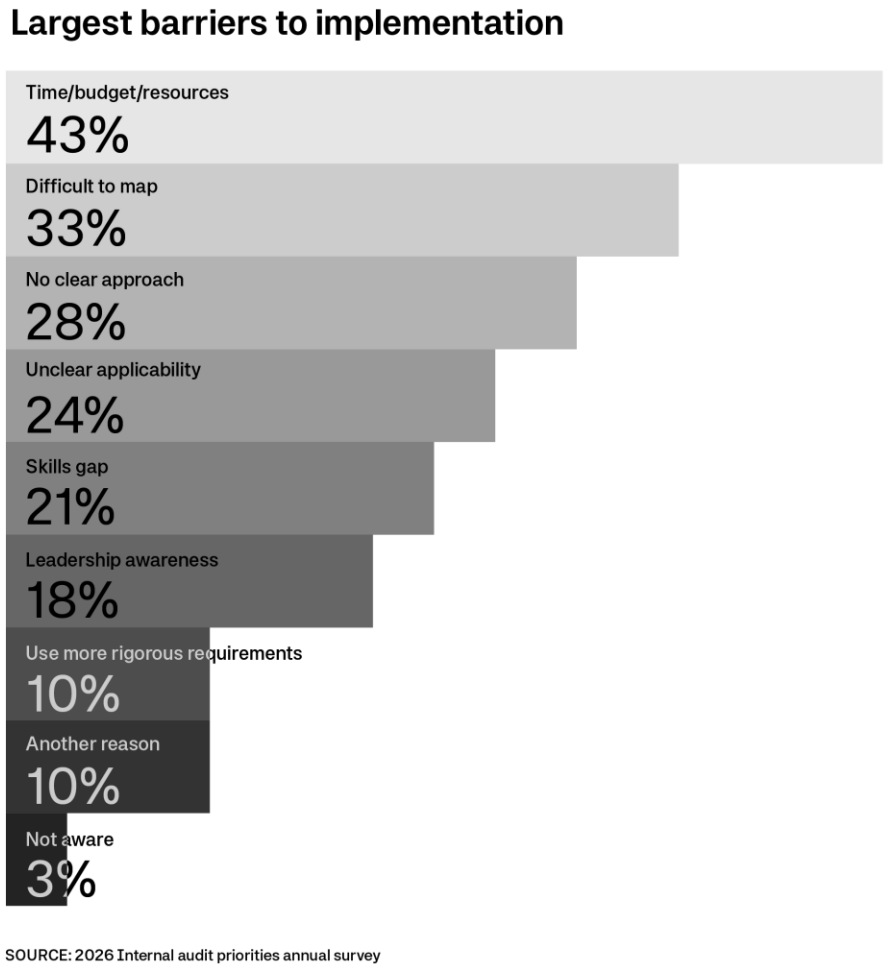


SOURCE: 2026 Internal audit priorities annual survey

Topical Requirements expose capacity and adoption concerns

Limited time, budget, and resources are the leading implementation barrier, cited by 43% of internal audit leaders. Internal audit leaders also report difficulty mapping the requirements to existing methodologies and determining when the requirements apply.

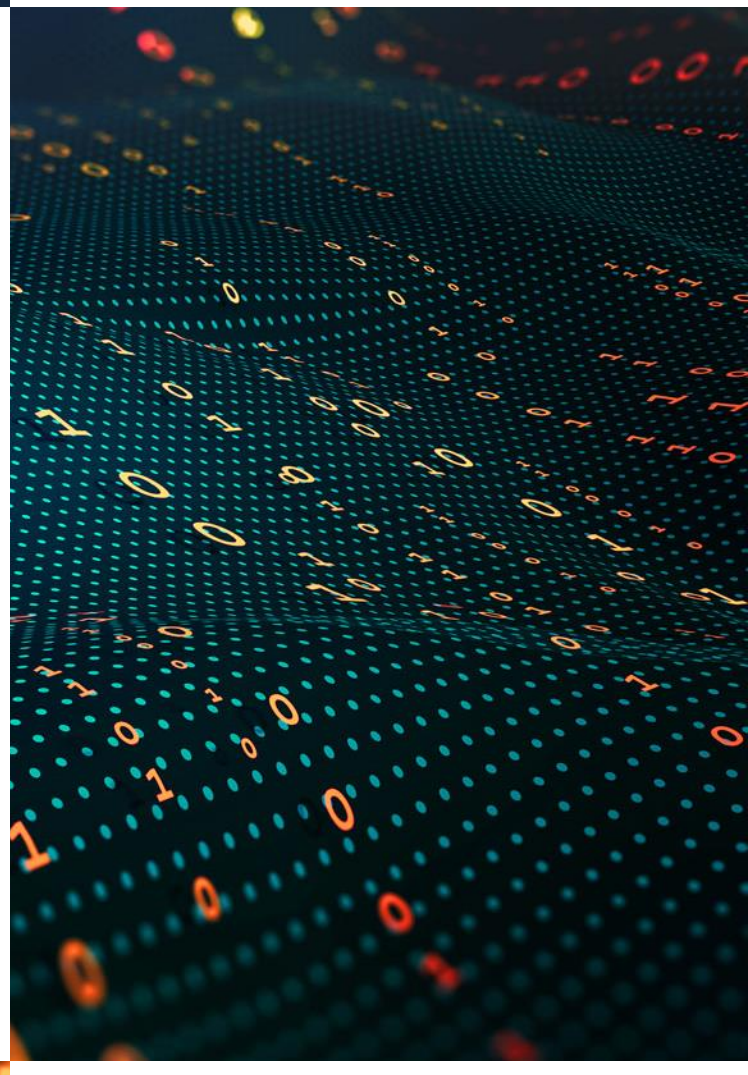
Implementation challenges span organizations of different sizes. Among organizations with $1 billion to $6 billion in annual revenue, 60% cite insufficient time, budget or resources, significantly higher than the 43% overall result. Meanwhile, smaller internal audit functions may find the minimum requirements disproportionately burdensome, particularly when they lack dedicated IT and cybersecurity resources. In practice, these functions may turn to external specialists when they do not have the capacity or technical expertise to complete applicable Topical Requirement assurance work internally.



SOURCE: 2026 Internal audit priorities annual survey

Cybersecurity and technology risk

Technology risk continues to become more deeply embedded across strategy, operations, data, third parties and organizational resilience.



Technology risk has expanded beyond the IT environment

Technology risk does not stop at the organization's network, systems, or legal boundaries.

Cybersecurity remains internal audit's leading emerging risk, but the scope of technology assurance continues to widen. Artificial intelligence, cloud services, data governance, identity and access, technology resilience, and third-party dependencies form an interconnected risk environment.

This expansion requires internal audit to look beyond individual technical controls. A cyber event may begin with an employee, a third-party provider, an unmonitored AI application, or a weakness deeper in the supply chain. Effective assurance must therefore consider how technology risk moves across organizational and vendor boundaries.

The results show encouraging growth in several areas of independent cyber assessment, including penetration testing, data loss prevention, and phishing programs. Yet coverage remains uneven, and 30% of respondents report that internal audit is not using cybersecurity tools directly.

The IIA's first two Topical Requirements reinforce the importance of this connected view of technology risk. The first addresses cybersecurity, while the second addresses third-party risk. Organizations increasingly obtain AI and other technology capabilities through outside providers, making vendor governance, SOC reporting, concentration risk, and downstream dependencies essential parts of the assurance landscape.

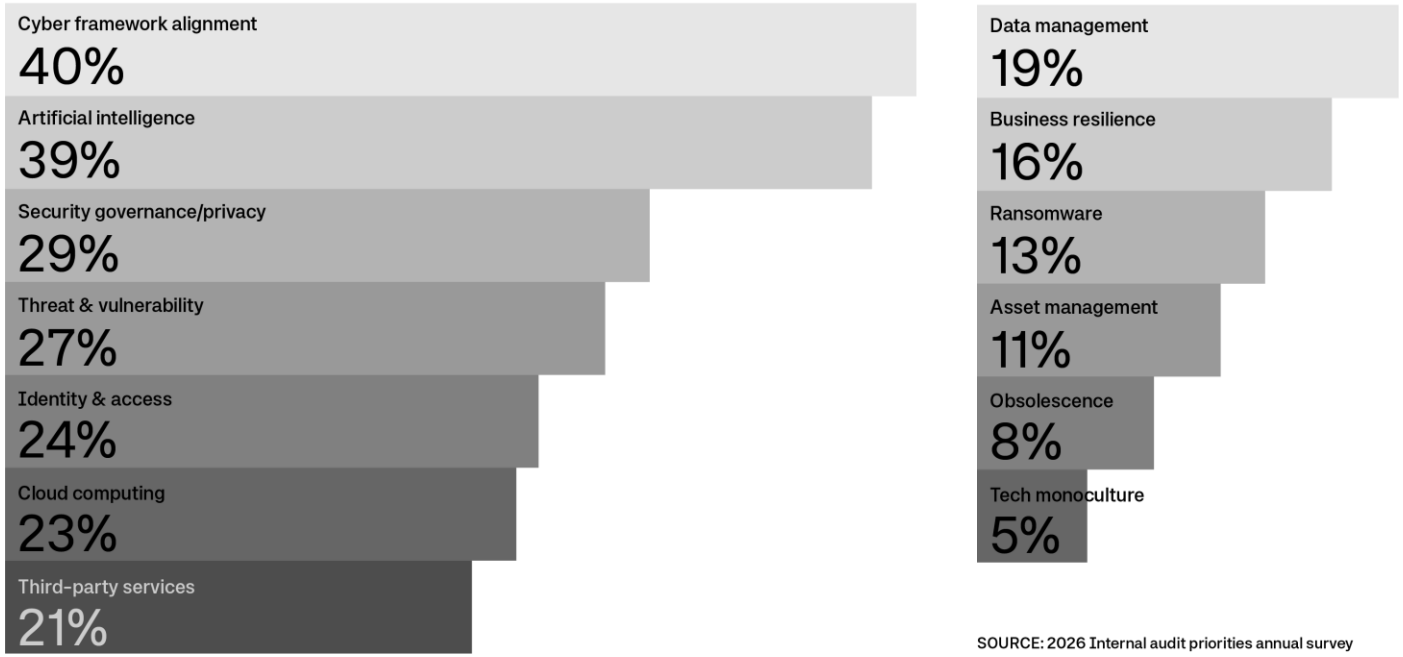
Technology risk assessments mirror the largest emerging risks

Alignment with established cybersecurity frameworks remains the leading priority in technology risk assessments, selected by 40% of internal audit leaders. Artificial intelligence follows closely at 39%, demonstrating how quickly AI has moved alongside traditional cybersecurity concerns as a central area of technology assurance.

Next, attention is spread across a wide range of interconnected risks. Security governance and privacy, threat and vulnerability management, identity and access, cloud computing, third-party services, data management, and business resilience all require focus, yet none was selected by more than 30% of respondents.

The results reflect the breadth of today's technology risk environment. Internal audit must assess not only whether cybersecurity controls align with recognized frameworks, but also how AI, data, cloud platforms, and external providers affect the organization's overall risk exposure. With so many technical areas competing for coverage, internal audit leaders must determine where deeper assurance and specialized support is most needed within the organization.

Priorities in the most recent technology risk assessment



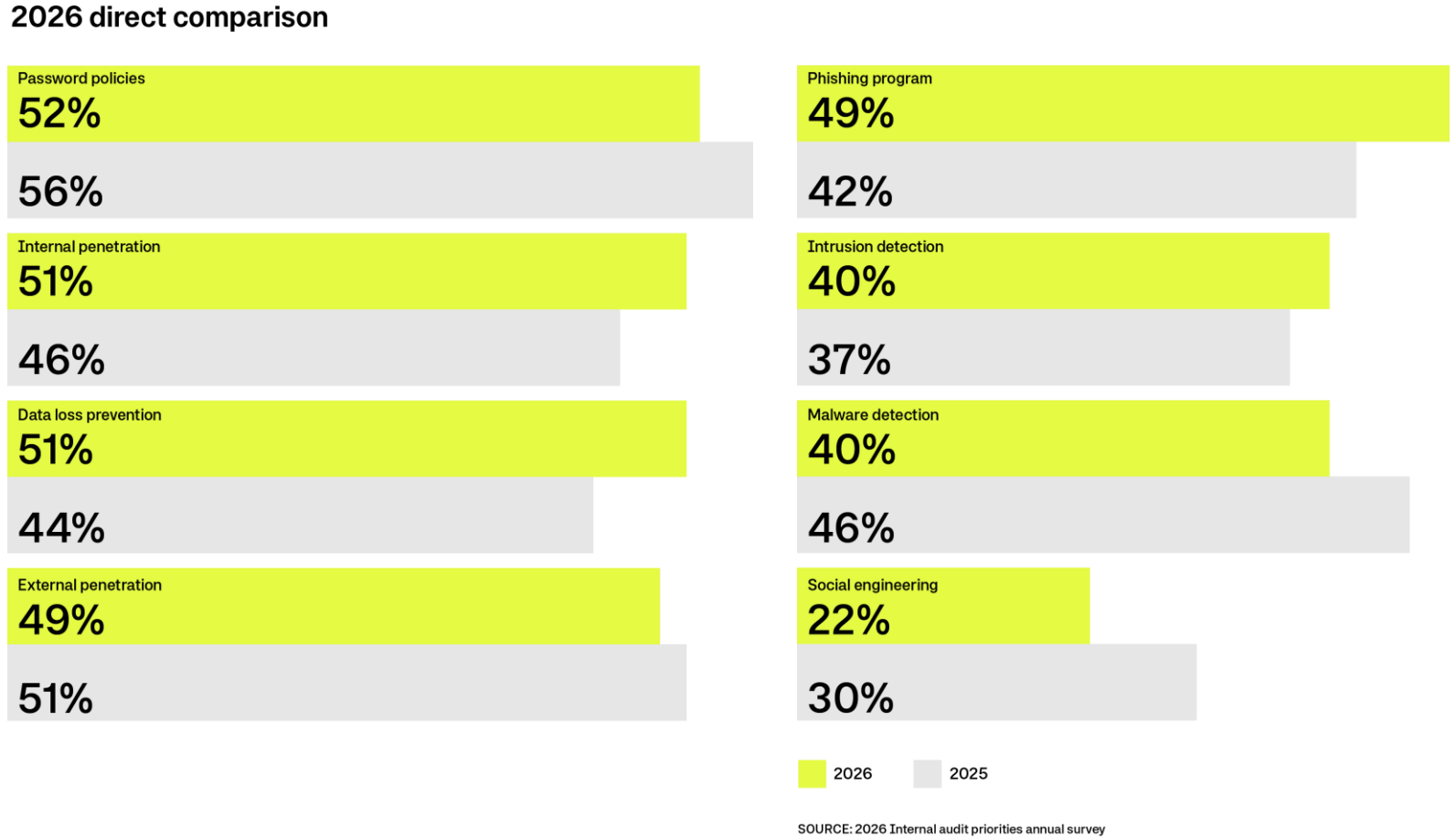
SOURCE: 2026 Internal audit priorities annual survey

Cyber assurance is broadening across controls

Internal audit's cybersecurity assurance is spreading across a core group of controls. In 2026, approximately half of internal audit leaders independently assessed password policies, penetration testing, data loss prevention, and phishing programs, suggesting that effective cyber assurance increasingly requires coordinated coverage across multiple control areas.

Data loss prevention and phishing-program assessments each increased seven percentage points from 2025, while internal penetration testing rose five points. However, malware-detection assessments declined from 46% to 40%, and social-engineering assessments fell from 30% to 22%.

These declines are notable as AI enables threat actors to develop more sophisticated phishing, impersonation, and other manipulation tactics at greater speed and scale. Cyber risk exposures may be evolving faster than internal audit functions and IT departments can adapt their controls and assurance activities. Internal audit functions may need to look beyond individual controls and assess whether technology, processes, and human behavior are keeping pace with a rapidly changing threat environment.



SOURCE: 2026 Internal audit priorities annual survey

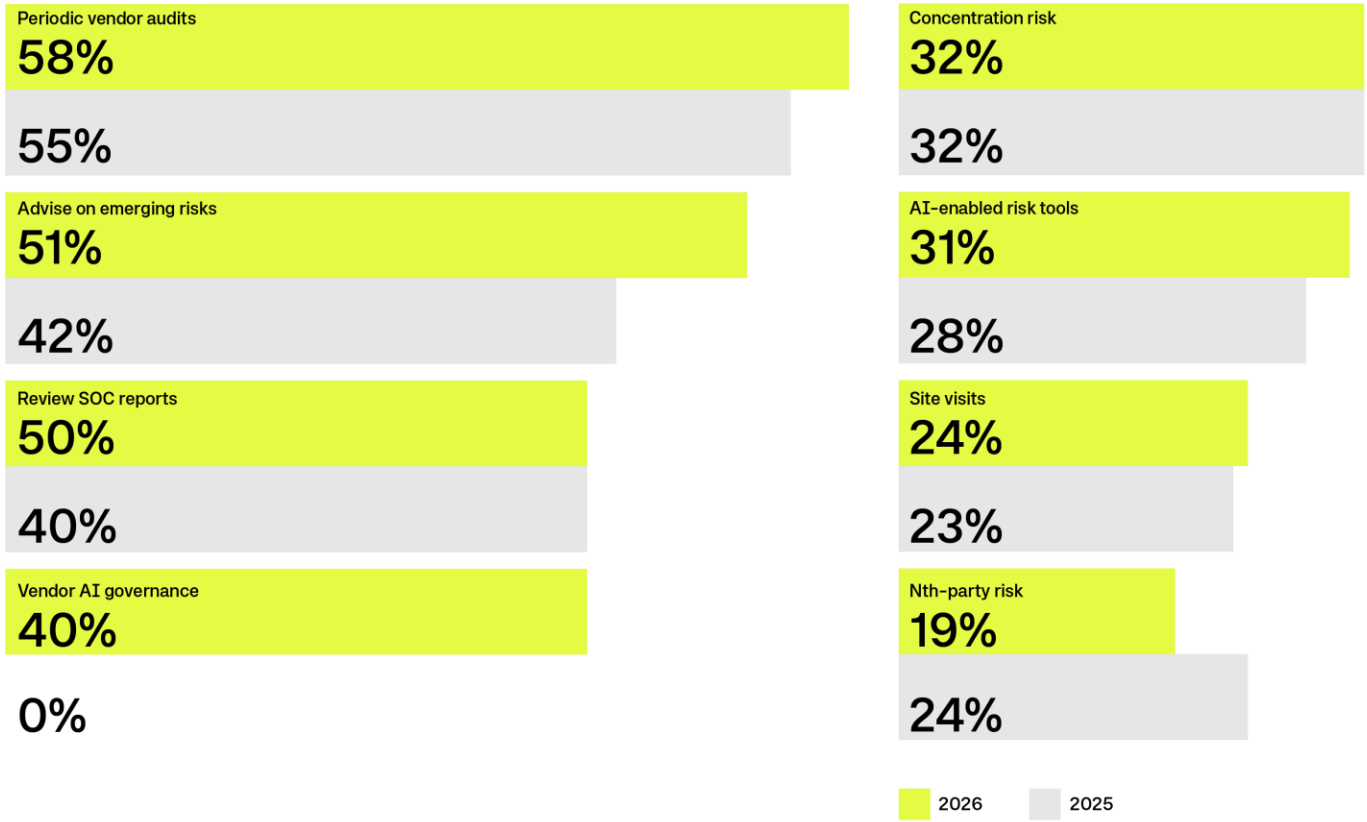
Third-party risk is absorbing new technology risks

Internal audit's role in third-party risk is expanding as vendors become more integrated into organizations' technology, data, and AI environments. Periodic vendor audits remain the most common activity, rising from 55% in 2025 to 58% in 2026.

The Institute of Internal Auditors' Third-Party Topical Requirement, effective September 15, 2026, establishes a mandatory baseline for assurance engagements involving third parties and downstream relationships. The survey results suggest that some internal audit functions are already broadening their approach. Advising on emerging third-party risks increased from 42% to 51%, while SOC report reviews rose from 40% to 50%. New in 2026, 40% also evaluate vendor AI governance, reflecting the growing use of AI by third parties, both in the services they provide and the capabilities they deliver to organizations.

However, only 19% evaluate Nth-party risks, down from 24% in 2025. Third-party risk exposure is likely to grow as vendors and their subcontractors incorporate AI into the products, services and business functions they deliver. The Third-Party Topical Requirement may create more focus on this evolving risk area by establishing a consistent baseline for assurance involving third parties and downstream relationships. As internal audit functions adopt the requirement, evaluation of Nth-party risks may increase, providing organizations with greater visibility beyond their immediate vendor relationships.

Internal audit's involvement in third-party risk



SOURCE: 2026 Internal audit priorities annual survey

Internal audit growth

Budgets and staffing are increasing, but not keeping pace with growing organizational risk.

Rising risk is driving internal audit growth

Internal audit is receiving more resources, but investment has not yet caught up with the function’s expanding mandate.

Internal audit growth reflects organizations' expanding risk exposure. Cybersecurity, artificial intelligence, regulatory requirements, third-party technology, and system implementations are creating demand for capabilities that many internal audit functions have not historically maintained at scale.

Nearly two-thirds of internal audit leaders report higher budgets, and 43% expect to increase headcount. However, additional investment has not eliminated the resource challenge. Internal audit leaders continue to report insufficient time, budget, and specialized skills as organizational risks become broader, more interconnected and more technically complex.

The central question is not only how many people the function employs. It is whether internal audit has the right combination of capacity, organizational knowledge, and technical capability to support effective risk mitigation and provide the assurance expected by management and the audit committee.

Investment is rising, but so is the capability challenge

Internal audit functions entered 2026 with more organizational support. Sixty-four percent report higher budgets and 43% expect to increase headcount. The greater investment in the internal audit function comes with heightened expectations for its capabilities and achievements.

Technical skills remain the leading hiring and retention challenge, as audit functions now compete directly with the broader technology market for cyber, AI, and data talent. Eighty-two percent of audit functions use external partners to supplement existing internal teams with specialized skills and flexible capacity. AI presents a similar challenge. Ninety percent of audit functions use AI, and most users report achieving their targeted return. However, assurance over organizational AI remains concentrated on governance, data, and security. Only 53% of audit functions assess operational effectiveness, while even fewer address bias or model validation.

Taken together, the results reveal the central tension of the 2026 report: internal audit is receiving more resources and adopting more technology, but expectations and the demands of addressing cyber, AI, and data risks continue to advance faster than the function's capabilities.



64%

Report increased budgets



82%

use external partners



90%

use AI in the audit function

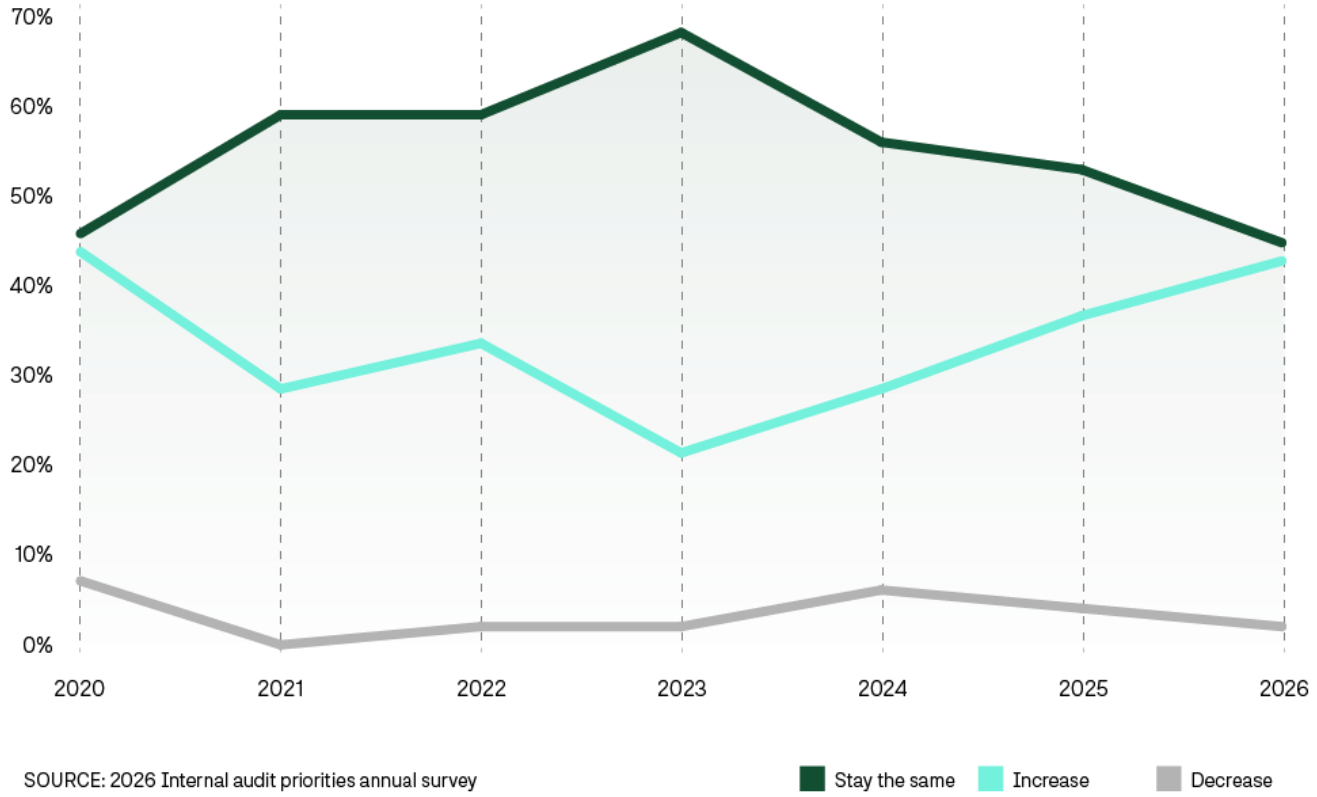
Headcount growth continues for a third year

Forty-three percent of internal audit leaders plan to increase headcount in 2026, up from 37% in 2025 and 29% in 2024. On average, functions expecting growth plan to increase budgets by 10.7%.

The three-year trend reflects sustained demand for additional internal audit capacity, but these figures represent hiring intentions rather than completed recruitment. Internal audit leaders must still compete for specialized cyber, AI, data, and technology skills that remain difficult to find and retain.

As a result, planned headcount growth may provide needed capacity without fully resolving the technical capability gaps facing many audit functions.

Forecast staffing direction for internal audit



SOURCE: 2026 Internal audit priorities annual survey

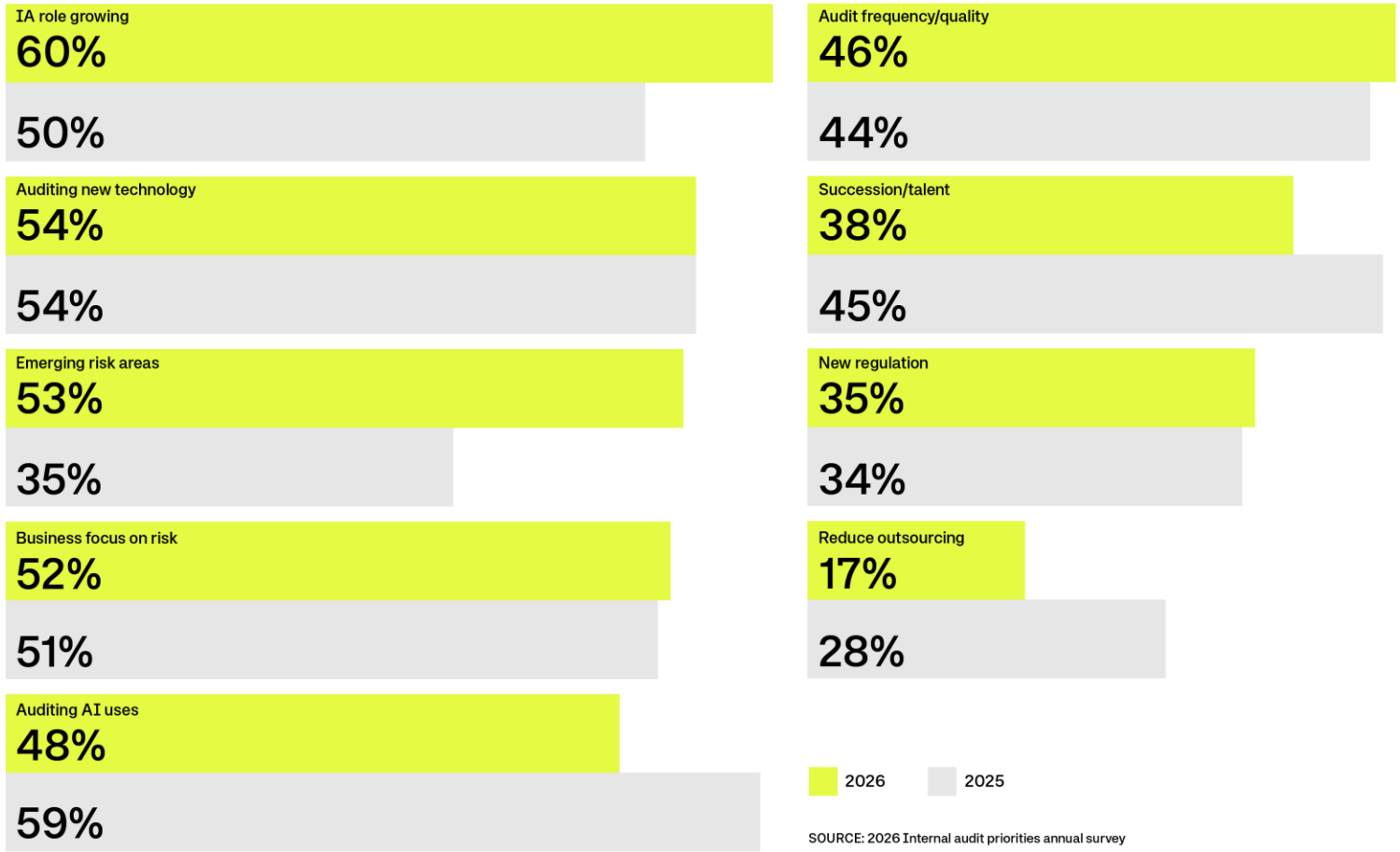
Internal audit is hiring because the role is expanding

Internal audit's expanding role is now the leading reason departments plan to hire. Among internal audit leaders expecting to increase headcount, 60% cite the function's growing role within the organization, up from 50% in 2025. The need to cover new emerging-risk areas also rose sharply, from 35% to 53%.

Technology continues to contribute to this demand. Fifty-four percent are hiring in response to increased auditing of new technology, unchanged from 2025. Increased auditing of AI declined as a stand-alone hiring reason, from 59% to 48%, but this does not necessarily signal lower demand for AI expertise. AI is increasingly embedded across technology implementations, third-party relationships, and other emerging-risk areas rather than treated as a separate category.

The challenge is not simply adding headcount, but building the capabilities needed to address a broader and more technically complex risk environment.

Why is your department planning to increase headcount?



SOURCE: 2026 Internal audit priorities annual survey

Talent

The talent challenge sits at the intersection of audit judgment, organizational knowledge, and technical specialization.



Internal audit is competing for a new kind of talent

The hardest profile to find is not a technologist or an auditor. It is a professional who can operate effectively as both.

The internal audit skills shortage is becoming more difficult as technology assumes a larger role in the audit plan. Cybersecurity, AI, data analytics, IT controls, and technology transformation are now among the most difficult capabilities to develop and retain.

These needs place internal audit in direct competition with information security, technology, data, and engineering functions. Professionals with the required technical knowledge can command compensation levels that may be difficult for audit departments to match, and internal specialists may be recruited into other parts of the organization.

Technical capability alone is not enough. Internal audit leaders also need professionals who understand the organization, apply sound judgment, communicate clearly with senior stakeholders, and translate technical findings into relevant business implications.

This creates a challenge across experience levels. Newer professionals may bring current technical knowledge but lack organizational context and stakeholder skills. Experienced auditors may understand the business but require substantial development in AI, cyber, and analytics.

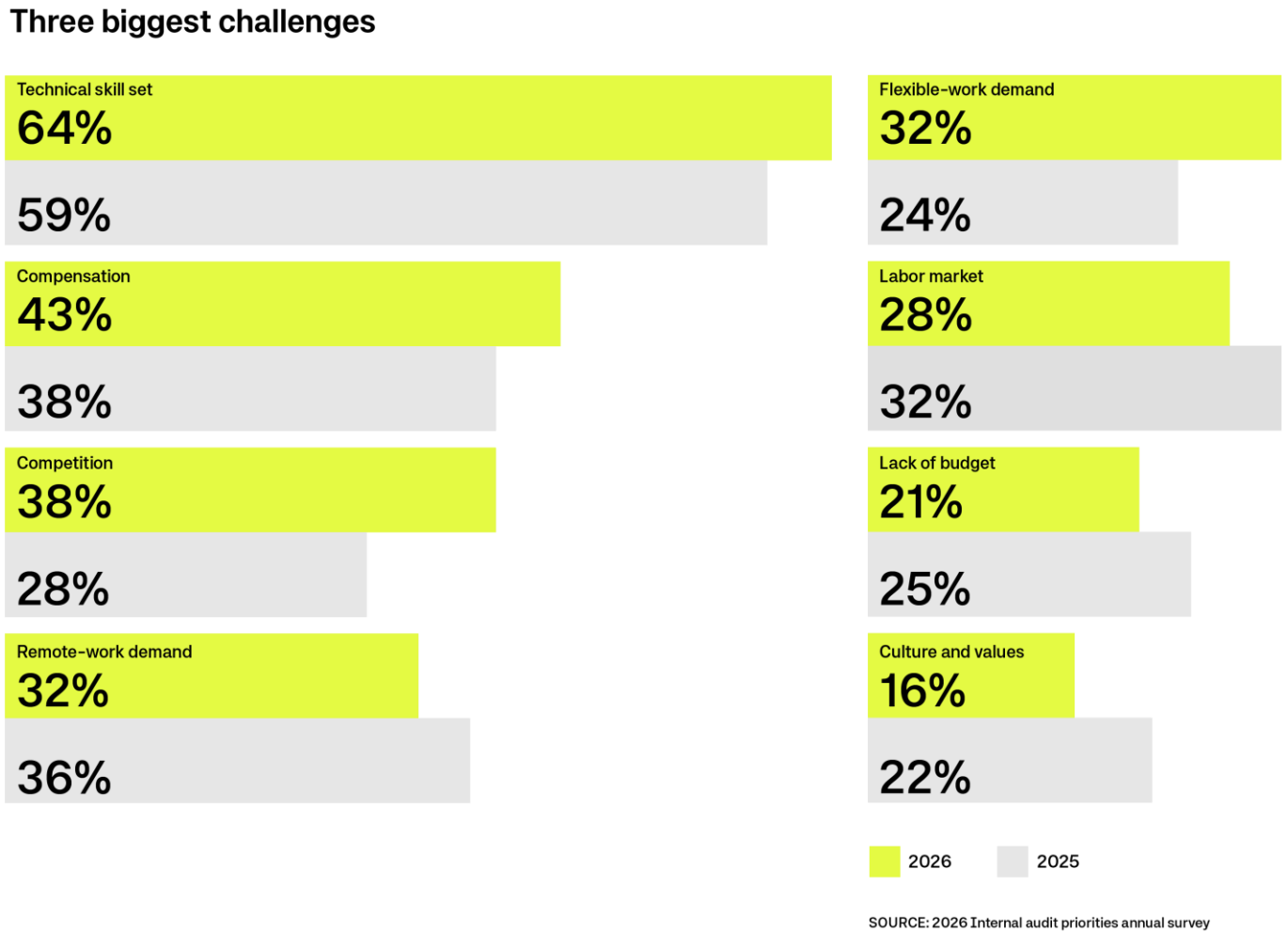
The most sustainable response will combine targeted recruiting, continuous development, internal mobility, and external specialization rather than relying on any single talent strategy.

Technical skills remain the largest hiring and retention barrier

Technical capability remains the leading challenge in hiring and retaining internal audit talent, increasing from 59% in 2025 to 64% in 2026. Compensation requirements also rose from 38% to 43%, while competition grew the most, climbing from 28% to 38%.

The results reflect a talent market in which internal audit is competing not only with other audit functions, but also with technology, cybersecurity, data, and operational teams for many of the same specialized skills. Meanwhile, more candidates are seeking flexible work arrangements, something employers should consider to maintain competitiveness.

The challenge is therefore broader than filling open positions. Internal audit leaders must offer competitive opportunities, continually develop existing teams, and create an environment where professionals can keep pace with rapidly changing technologies and risks.



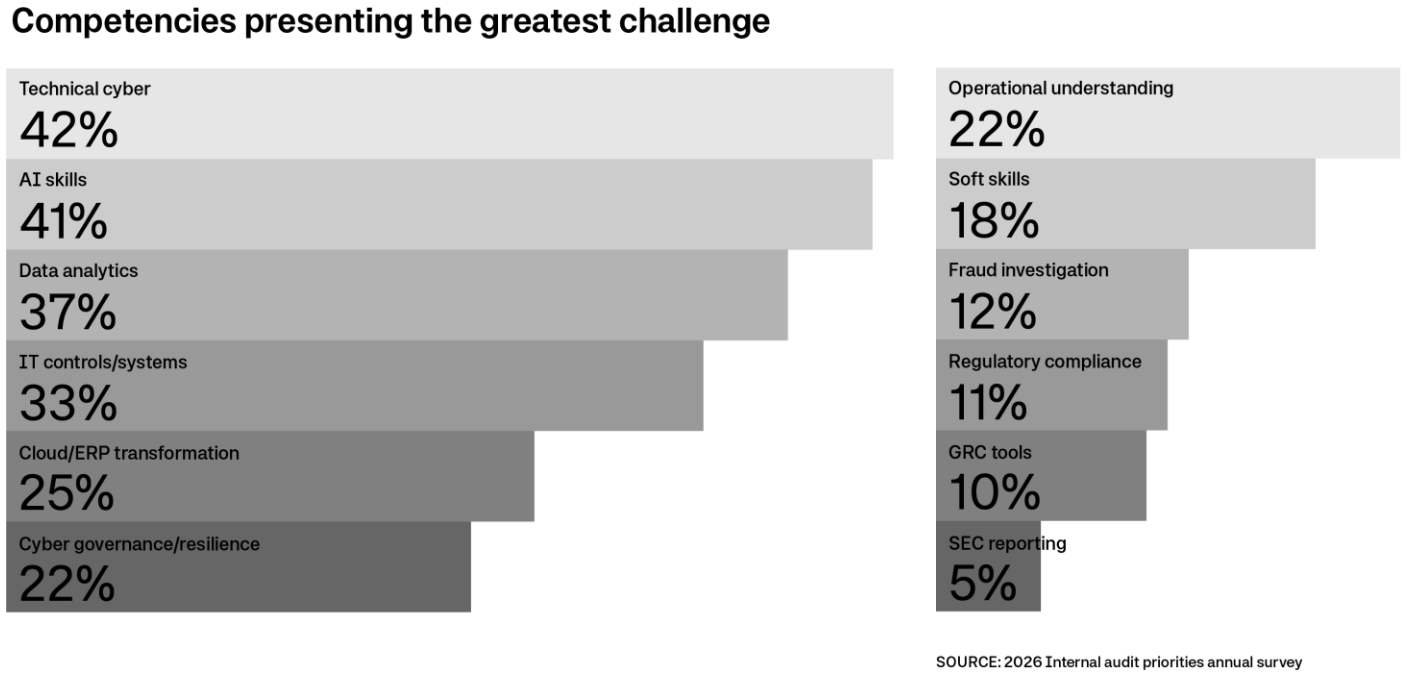
SOURCE: 2026 Internal audit priorities annual survey

Cyber and AI skills are the hardest to develop and retain

Cybersecurity and AI capabilities are the most difficult skills for internal audit functions to develop and retain, cited by 42% and 41% of internal audit leaders, respectively. Data analytics follows at 37%, while one-third identify IT controls, systems, and infrastructure auditing as a challenge.

These findings reflect both the specialization required and the speed at which the underlying technologies continue to change. Audit functions must invest continually in training and development, yet employees with these capabilities are also in demand across cybersecurity, technology, data, and operational teams.

Technical knowledge alone does not resolve the challenge. Internal audit also needs professionals who understand the organization, apply auditor judgment and communicate technical findings in a way that supports business decisions. Building that combined skill set takes time, making it especially difficult to develop internally and retain over the long term.



SOURCE: 2026 Internal audit priorities annual survey

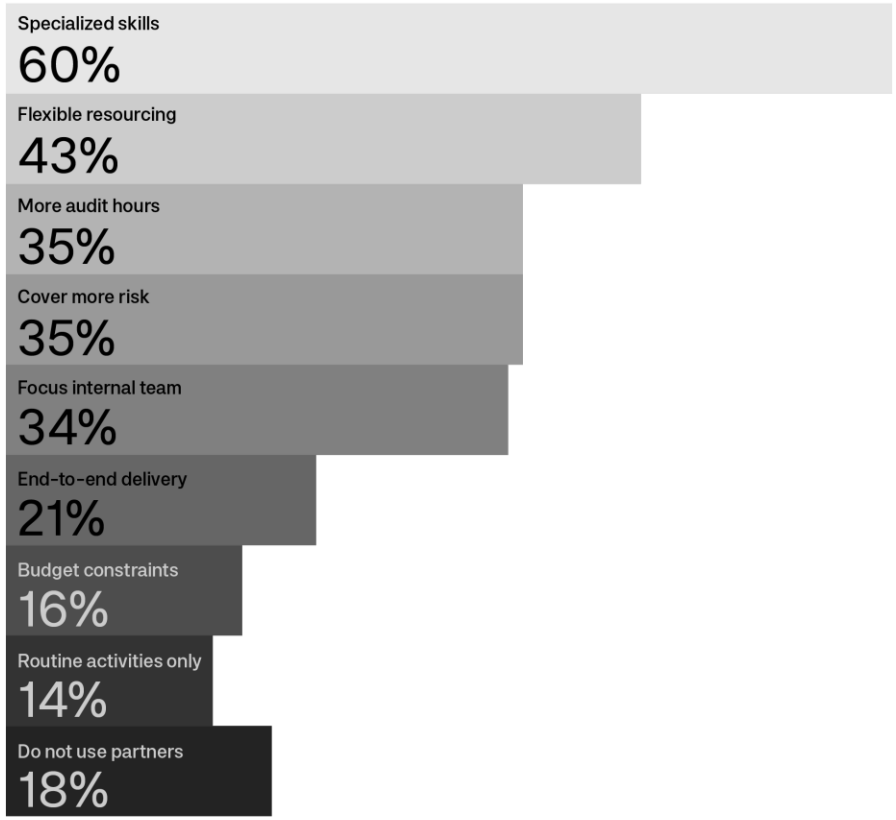
External partners have become part of the operating model

External partners have become a significant part of the internal audit operating model, with 82% of internal audit leaders reporting that their functions use external, offshore or global delivery resources. Sixty percent of respondents cited access to specialized skills as the primary reason, especially as organizations struggle to maintain expertise in cybersecurity, AI, data analytics, and other technical areas internally.

Audit functions also use external partners to respond more flexibly to changing demands. Forty-three percent cite the ability to scale resources up or down, while approximately one-third use partners to increase available audit hours, cover more areas of risk, or allow internal teams to concentrate on priority work.

The findings suggest that external support is no longer used only to address vacancies or short-term capacity constraints. Internal audit leaders are increasingly combining the organizational knowledge and judgment of internal teams with specialized expertise that can be added as risks, technologies, and assurance needs evolve.

Reasons internal audit uses external, offshore or global delivery partners



SOURCE: 2026 Internal audit priorities annual survey

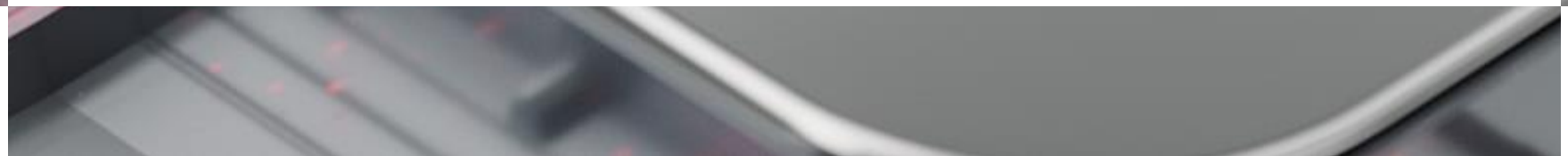


Artificial intelligence

AI is both a major audit subject and an increasingly embedded tool across the audit lifecycle.







AI adoption is advancing faster than AI assurance

AI has moved into the audit workflow faster than assurance practices have matured around it.

Artificial intelligence has moved quickly from an emerging technology to an embedded part of internal audit work. As its use expands across the audit lifecycle, internal audit functions must consider both how they govern AI within their own work and how they provide assurance over its use across the organization.

This expansion offers meaningful efficiency and capacity benefits. Ninety percent of respondents report using AI within the audit function, and 82% of those users say the technology is achieving its targeted return on investment.

However, the survey also reveals a potential assurance gap. AI audits are heavily focused on governance, data privacy, inventories, and cybersecurity. Operational effectiveness, ethical use, bias, and model validation receive considerably less attention.

The distinction between safe AI and effective AI may be misleading. A model that is well governed but produces inaccurate or biased decisions can still create significant risk. As AI becomes more central to operations and assurance work, internal audit will need to examine not only who owns the technology and how it is controlled, but whether it produces reliable and appropriate outcomes.

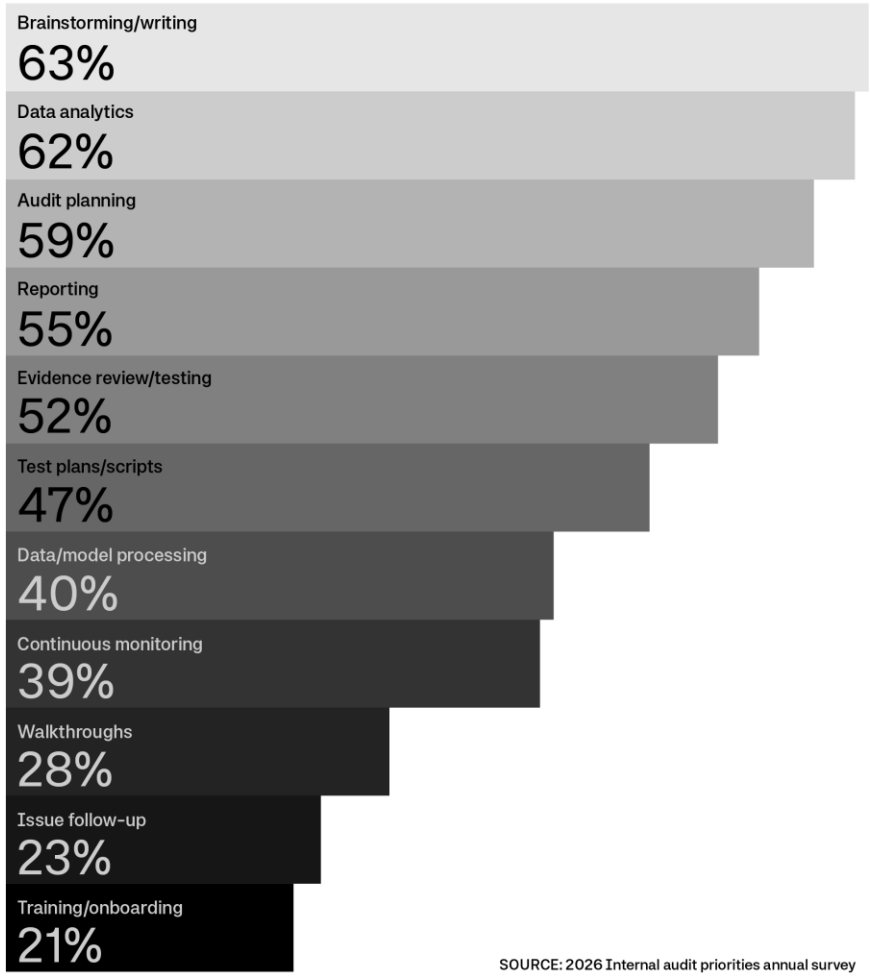
Ownership remains unsettled as well. Larger organizations are more likely to rely on dedicated AI steering committees, while smaller organizations assign primary responsibility to internal audit more frequently. This may address an immediate governance need, but it can create independence concerns when audit later assesses the structure it owns.

AI is moving into core audit work

AI usage among respondents now extends beyond writing and brainstorming. More than half use AI for analytics, planning, reporting and evidence review, or control testing.

As AI influences audit scope, procedures, and conclusions, functions need clear expectations for validation, documentation, human review, and data protection.

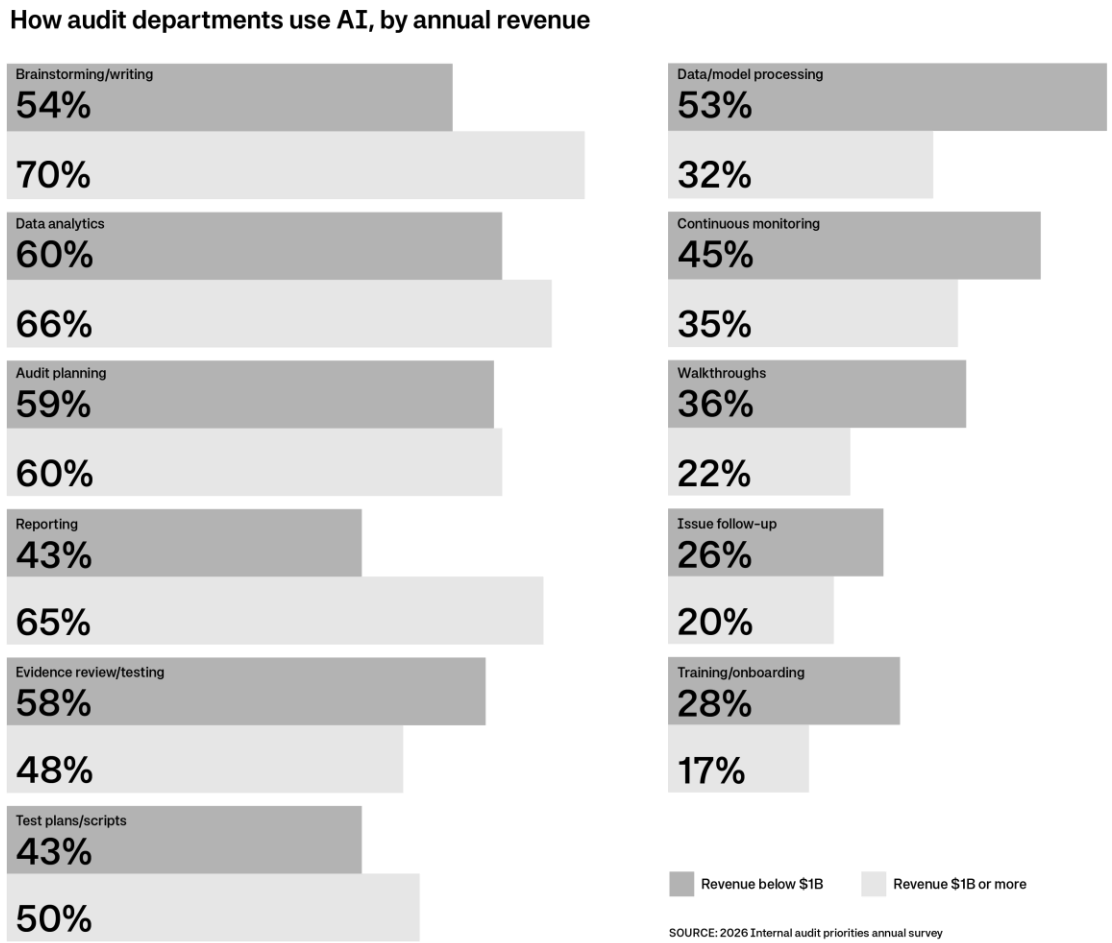
How audit departments use artificial intelligence



SOURCE: 2026 Internal audit priorities annual survey

AI use differs by organization size

Larger organizations more often use AI for writing, reporting, and test-plan development. Smaller organizations report higher use for evidence review and testing, data and model processing, continuous monitoring, and walkthroughs.



AI adoption is outpacing the assurance conversation

Ninety percent use AI, exceeding the 84% using internal audit-specific software. Among AI users, 82% report achieving targeted ROI. Reported AI ROI also varies by organization type and revenue, although the available results do not show whether those differences reflect adoption rates, realized returns or both. Because respondents defined ROI for themselves, the result should be viewed as directional. Internal audit leaders should establish how productivity, quality, capacity and cost benefits are measured consistently.



90%

currently use AI within their audit function

82%

of those say that it is achieving targeted ROI



84%

currently use internal audit-specific software

87%

of those say that it is achieving targeted ROI



74%

currently use AI functionality within internal audit-specific software

75%

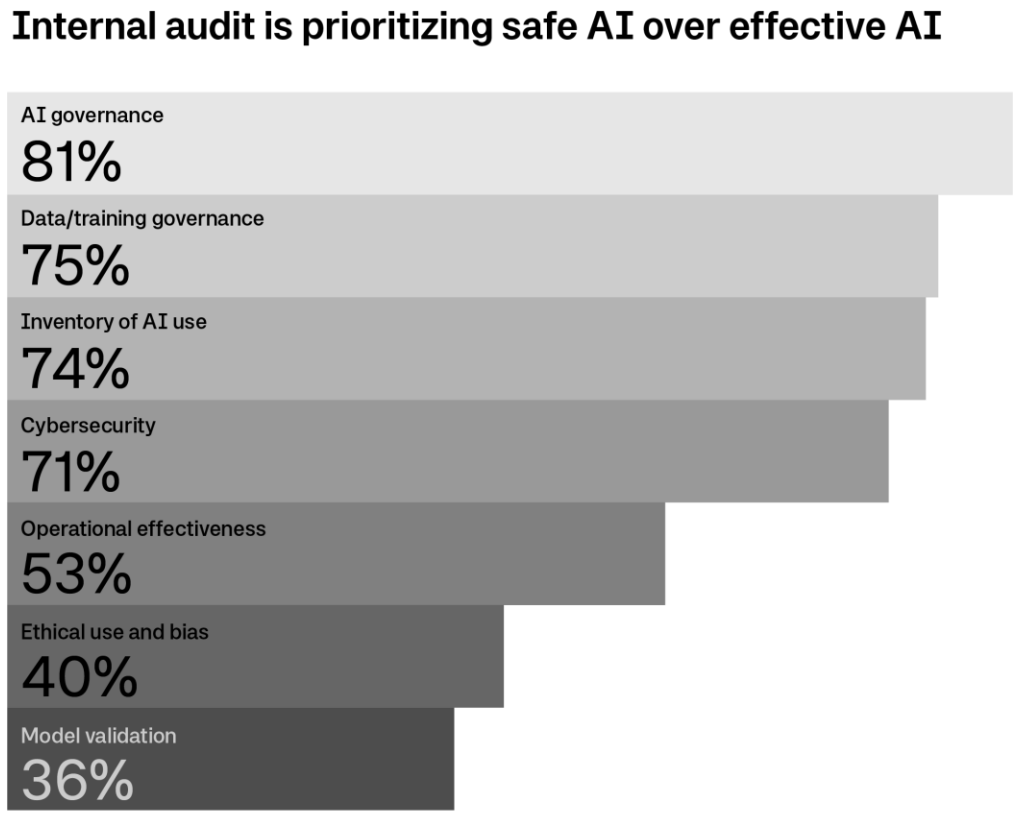
of those say that it is achieving targeted ROI

Internal audit is prioritizing safe AI over effective AI

AI governance, data privacy, inventories of AI use, and cybersecurity currently lead the assurance agenda. These areas are essential for establishing accountability and protecting the organization, but they do not fully address whether AI is producing accurate, reliable and appropriate results.

Only 53% of respondents auditing AI review operational effectiveness, while 40% address ethical use and bias and 36% include model validation. If an AI model produces inaccurate or biased decisions, the organization may still face significant risk, even when governance and security controls are in place.

As AI becomes more embedded in business operations, internal audit will need to expand assurance beyond governance and safety to include model performance, decision quality, and intended outcomes.



SOURCE: 2026 Internal audit priorities annual survey

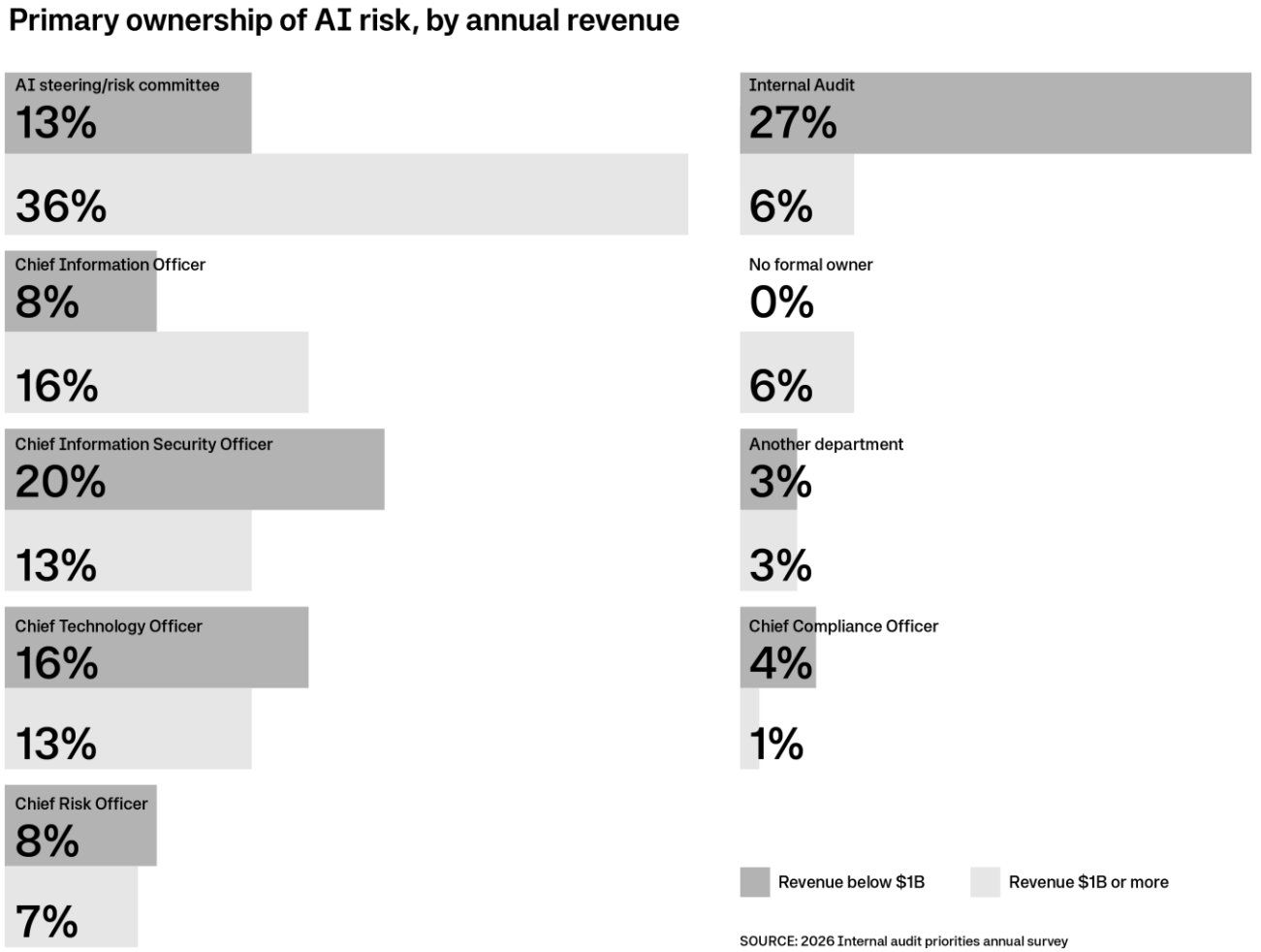
AI ownership remains unsettled

AI risk ownership is distributed across a wide range of functions, reflecting the cross-functional nature of AI governance. Organization size significantly affects how AI risk ownership is structured. Thirty-six percent of organizations with at least $1 billion in revenue assign ownership to an AI steering or risk committee, compared with only 13% of organizations below $1 billion.

Internal audit is the primary owner in 27% of smaller organizations, compared with only 6% of larger organizations. Smaller companies may have fewer dedicated risk, technology, or governance resources, causing responsibility to fall to the function most prepared to evaluate controls.

This approach may address an immediate governance need, but it also creates an independence concern. Internal audit should not design, own, and later provide assurance over the same AI governance structure.

Smaller organizations may not require a large or formal committee, but they still need clearly assigned management ownership, cross-functional participation, and an independent role for internal audit. Primary ownership should generally remain with management so internal audit can assess accountability, challenge governance effectiveness and provide independent assurance.



Conclusions

What the findings mean for internal audit leaders

The 2026 findings point to a function at an important stage in its evolution. Internal audit is receiving more investment and taking on broader responsibilities, but increasing budgets and headcount will not close every capability gap. The risks creating the greatest demand are also among the fastest-moving and most technically specialized.

Internal audit leaders will need to make deliberate choices about where the function can provide the greatest value. Organizational knowledge, auditor judgment, and trusted relationships should remain central to the internal audit model. Specialized external support can complement those strengths with technical expertise and flexible capacity in areas such as cybersecurity, AI, and third-party risk.

The scope of assurance must also continue to evolve. Technology and AI risks increasingly extend beyond the organization through vendors, data providers and other external dependencies. Looking ahead, increasingly autonomous AI, more sophisticated AI-enabled cyber threats and deeper reliance on interconnected third-party technologies may further challenge traditional approaches to governance and assurance. Data security and privacy risks may also grow as employees and third parties use AI tools to access, process or share organizational data in ways the organization has not authorized or cannot see. Internal audit functions will need to assess not only governance and security, but also how data is used and protected and whether AI models are accurate, reliable, unbiased and operating as intended.

The opportunity is not to cover every emerging risk with equal depth. It is to align the audit plan with the risks that matter most, build or obtain the capabilities needed to assess them, and connect near-term assurance work to the organization's longer-term strategy and resilience.

Internal audit's relevance will be measured not by how much work the function adds, but by the confidence its assurance gives leaders navigating change.

Sikich at a glance

Sikich offers the public and private sectors a diverse platform of professional services across consulting, technology and compliance. Highly specialized and hands-on teams deliver integrated solutions rooted in deep industry experience. Our approach is strategically and thoughtfully designed to help our clients, teams and communities accelerate success.

About the research

The 2026 Internal Audit Priorities Survey is the tenth annual study examining the risks, operating challenges and evolving responsibilities of internal audit leaders in the United States. Sikich, using the services of research consultancy Reputation Leaders, conducted an online study among 222 U.S. audit leaders. Public companies represented 54% of respondents, while 35% worked for privately held organizations. Respondents represented audit functions of varying sizes and organizations across a broad range of annual revenue. Fieldwork took place between July 24 and August 19, 2026.