NAVIGATING A TECHNOLOGY RISK-FILLED HORIZON

Assessing the results of the Global Technology Audit Risks Survey conducted by Protiviti and The Institute of Internal Auditors

The Institute of Internal Auditors

protiviti®
Global Business Consulting

Table of Contents

Introduction

Protiviti partnered with The Institute of Internal Auditors (The IIA) to conduct its 11th annual Global Technology Audit Risks Survey in the second and third quarters of 2023. The objective of this survey is to explore the top technology risks organisations face, as perceived by technology audit leaders and professionals. Additionally, it explores the practices, processes and tools employed to help enterprises identify, manage and mitigate these risks. A total of 559 executives and professionals, including chief audit executives (CAEs) and information technology (IT) audit directors, completed the online survey.

This report, summarising the survey results, functions as both a mirror and a roadmap. It provides insights into the current state of technology risks while also guiding technology audit leaders and teams through the challenges and opportunities that lie ahead. Additionally, within the report, we offer key calls to action aimed at assisting IT audit leaders and teams in taking their technology audits to the next level.

"When it comes to technology challenges, not only are companies facing a wide range of threats, but each of these threats also is changing at an alarming rate. Risks related to cyber and AI look radically different than a few years ago, and will surely continue to evolve. Companies that conduct internal audits more frequently and integrate advanced analytical tools and techniques into their audit processes will be more on top of these changes and consequently more prepared when real issues arise."

— Angelo Poulikakos, Managing Director,
Global Leader, Technology Audit and Advisory practice, Protiviti

Executive summary and key findings

The results from this year's Global Technology Audit Risks Survey reveal a complex and multifaceted landscape of technology risks.

Cybersecurity is the top priority … and by a wide margin.

- Nearly 75% of all respondents and even more CAEs and technology audit leaders consider cybersecurity to be a high-risk area.
- Moreover, respondents believe next-gen cyber threats pose the most significant risks over the next two to three years.

Artificial intelligence (AI) is an emerging risk with gaps in organisational preparedness and audit proficiency.

- While only 28% of respondents indicate AI (including generative AI) and machine learning (ML) pose significant threats to their organisation over the next 12 months, AI is rated among the emerging technologies posing the most significant risks over the next two to three years. This suggests that while AI may not be perceived as an immediate threat, it is rising rapidly on the risk horizon.
- As AI adoption is set to soar, it represents a latent risk that organisations must start preparing for now. Few organisations believe their level of preparedness or the proficiency of their technology audit group in handling AI and ML risks are at acceptable levels.

Our key findings

- Cybersecurity is the top priority … and by a wide margin.
- AI is an emerging risk with gaps in organisational preparedness and audit proficiency.
- The talent gap in IT is a growing concern.
- Data privacy is a growing regulatory challenge.
- Data governance and transformation are of significant concern.
- Navigating the complex landscape of third-party and vendor risk is a challenge.
- More frequent auditing drives risk preparedness.

The talent gap in IT is a growing concern.

- While respondents report that their IT audit teams are moderately proficient at effectively evaluating IT talent management and the perceived threat associated with attracting, developing and retaining skilled technology personnel ranks in the middle of the pack compared to other risks, enterprise preparedness remains relatively low.

Data privacy is a growing regulatory challenge.

- Data privacy regulations such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and forthcoming legislation in other jurisdictions are adding layers of complexity to technology risk management. Our survey shows that while many respondents are confident in their organisation's cybersecurity measures, fewer are equally confident in data privacy compliance.

Data governance and transformation are of significant concern.

- CAEs and IT audit leaders are concerned about ensuring the accuracy, consistency and trustworthiness of their data. Proper data governance is not just a compliance requirement — it also represents the foundation for successful digital transformations and AI initiatives.

Navigating the complex landscape of third-party and vendor risk is a challenge.

- Global events such as supply chain disruptions and regulatory changes, combined with the increased use of cloud services and other outsourced IT functions, have amplified the importance of vetting third-party providers. This screening extends beyond cost effectiveness to encompass compliance with security and data protection standards.

More frequent auditing drives risk preparedness.

- Our survey results demonstrate a clear connection between the number of technology audits performed annually and an organisation's ability to manage critical technology risks.

Resources offered by The IIA

For relevant IT auditing guidance, we encourage you to explore the valuable resources provided by The Institute of Internal Auditors:

Auditing IT Governance

Assessing Cybersecurity Risk

Auditing Cybersecurity Operations: Prevention and Detection

Auditing Cyber Incident Response and Recovery

Auditing Third-Party Risk Management

Data Analysis Technologies

Call to action — elevate your technology audits

If you take only one action based on the findings of this research, consider increasing the frequency of your technology audits. If you can make another move, consider deploying (or increasing) the use of data analytics on technology audits.

These two activities correspond to a wide range of positive technology audit outcomes. These outcomes include more timely snapshots and deeper insights into both traditional and newly relevant technology risks. Additionally, they contribute to improved organisational preparedness and technology audit proficiency to address cybersecurity, regulatory compliance, data privacy and compliance, data governance, third-party risk management (TPRM), IT talent management, AI-related risk management, and more.

Below is a detailed rundown of high-level actions for technology audit teams to consider:

- **Increase audit frequency for high-impact areas,** especially those areas identified as critical emerging risks, to maintain a pulse on rapidly evolving challenges. Our results reveal that a higher number of technology audits conducted annually is associated with better risk awareness. Increase the frequency of audits in the areas identified as emerging risks to maintain a pulse on rapidly evolving challenges.
- **Maintain vigilance,** even over risks that the organisation is well-prepared to manage. It's tempting to become complacent in areas where the threat is high but the organisation feels ready to manage. Conduct audits in these areas regularly to ensure preparedness measures remain effective, and update risk mitigation strategies, as necessary.
- **Leverage advanced analytics for deeper insights,** integrating these tools and techniques into audit processes to better understand risks and the effectiveness of current risk management strategies. Given the complexity of today's risk landscape, basic auditing methods may not suffice.
- **Assess perceived threat levels** of technology audit risks in conjunction with organisational preparedness and internal audit's proficiency concerning each threat; this multidimensional "threat grid" evaluation strengthens priority-setting and produces more targeted audits.
- **Seek new ways to help improve** organisational preparedness regarding two high-threat areas: TPRM and IT talent management.

- **Improve internal audit's ability** to address IT talent management issues that pose significant risks to the organisation, the internal audit function and the technology audit group.
- **Recognise** that most leadership development and succession planning capabilities — organisationally and within the audit group — require more time from current leaders and more transparent communications with rising leaders.
- **Prioritise next-gen cyber threats** today. Given the widespread concern regarding next-generation cyber risks, technology audit teams should collaborate actively with their cybersecurity counterparts to assess organisational preparedness. This assessment should include evaluating the effectiveness of current threat detection mechanisms, the readiness to handle sophisticated cyber attacks like zero-day exploits and the measures in place for real-time threat intelligence sharing. Audit teams also should confirm that incident response plans are updated to address emerging types of cyber threats effectively.
- **Act now on AI,** including generative AI, and ML risks. Organisational use of these technologies is increasing rapidly and evolving in unexpected ways, while AI-related organisational preparedness and technology audit proficiency remain low. With advanced AI systems posing significant risks, the need for robust AI governance has never been greater. Start by developing ethical guidelines and control frameworks specifically for AI.
- **Revisit cloud security policies,** making sure to include aspects like data residency, encryption and access controls as part of this review.
- **Exert internal audit's** direct and indirect influence to address the most significant barriers — budgets, access to technical skills, return on investment (ROI) quantifications — hindering the adoption of advanced auditing technologies and tools.
- **Strengthen collaboration** with technology (CIO) and cybersecurity (CISO) teams, relationships with external partners, and recruiting and retention activities to improve the technology audit team's ability to manage current and emerging technology risks.
- **Invest in upskilling,** especially for emerging technologies. Lack of technical skills is a technology adoption barrier for many technology audit functions. A rapidly evolving technological landscape requires a skilled technology audit team, especially in areas like AI and ML. Identify skill gaps and invest in targeted training programs to ensure the technology audit team is equipped for future challenges.
- **Integrate environmental, social and governance (ESG) risks** into audit plans. With a growing focus on ESG risks related to technology, it's time to integrate ESG considerations into the technology audit framework. This integration will help the organisation stay ahead of regulatory changes and societal (including customer and stakeholder) expectations.

Definitions of survey-assessed technology risks

In this year's Global Technology Audit Risks Survey, we assessed 13 different technology risks that organisations face. Below is the list of these technology risks, along with their respective definitions.

AI & machine learning (including generative AI) — Risks from ethical concerns, security breaches, and operational issues in AI/ML applications, including large language models like GPT.

Cloud computing — Risks of data breaches, loss of data control, and non-compliance in cloud-based solutions.

Cybersecurity — Risks from unauthorised access, disruption, or destruction of information, systems, or networks.

Data governance & integrity — Risks related to maintaining accurate, consistent, and reliable enterprisewide data.

Data privacy & compliance — Risks in protecting personal data and keeping up with evolving data protection regulations.

IoT (Internet of Things) — Risks from vulnerabilities in connected devices and networks leading to potential breaches.

IT talent management — Risks associated with attracting, retaining, and developing skilled IT personnel, impacting operational efficiency and innovation capacity.

Modern software development — Risks associated with modern software development and deployment, such as DevOps, CI/CD, and containerisation.

Regulatory compliance — Risks related to adhering to industry-specific regulations governing technology use.

Technical debt & aging infrastructure — Risks from outdated systems leading to inefficiencies, vulnerabilities, and costly future updates.

Technology resiliency — Risks associated with maintaining adaptability and recovery capabilities in the face of IT disruptions or outages.

Third parties/vendors — Risks related to the security, reliability, and resilience of third parties.

Transformations & system implementations — Risks involving major business or IT changes, including disruptions, unmet requirements, data loss, etc.

Evaluating technology audit frequency

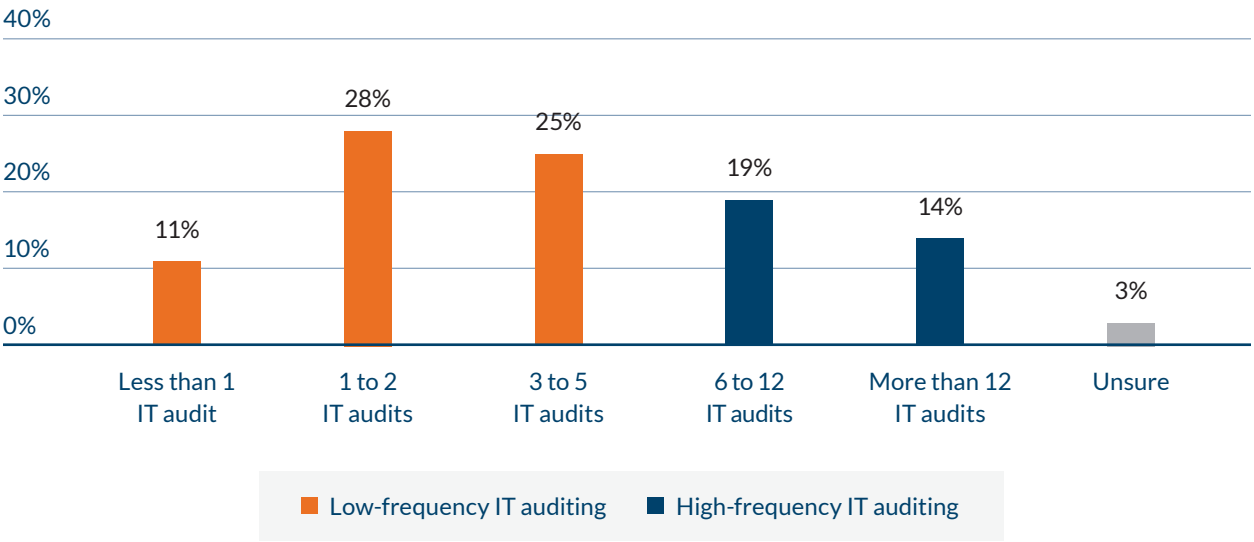
A metric we examined in this year's Global Technology Audit Risks Survey is how often organisations conduct technology audits. To facilitate our analysis, we categorised the received responses into two distinct groups:

- **High-frequency IT auditing** — Organisations that conduct six or more technology audits per year
- **Low-frequency IT auditing** — Organisations that conduct five or fewer technology audits per year

These high- and low-frequency IT auditing groups are referenced throughout our report. As illustrated in Figure 1 below, the majority (64%) of respondents indicate that their organisations perform five or fewer technology audits per year.

Number of technology audits performed per year

Figure 1



Question: *On average, how many IT audits does your organisation perform per year? Please exclude ongoing IT compliance work (e.g., IT SOX testing). n=559.*

Why frequency matters

- **Preparedness.** Our survey results suggest that organisations in the high-frequency IT auditing category are generally better prepared to manage a broader spectrum of technology risks (see Figure 5).
- **Utilisation of technology tools.** High-frequency IT auditors commonly employ next-generation audit tools and technologies, potentially enhancing their ability to identify, manage and mitigate related risks (see Figure 10).
- **Risk awareness.** The frequency of audits appears to influence the perception of near-term technology risks (see Figure 3).

By taking into account the frequency of your organisation's technology audits in relation to these factors, you can gain additional insights into your current risk posture and identify areas for potential improvement. Therefore, frequency is not just a number; it also provides a lens through which to view and understand the complex landscape of technology risks your organisation faces as well as emerging risks on the horizon.

"Technology and its associated threats are reshaping the landscape for audits and auditors. Rapid advancements in AI, data analytics, and automation bring opportunities for organisations and audit functions alike, but they also come with risks such as data breaches and cybersecurity threats. As technology continues to evolve, internal auditors must acquire the skills necessary to continue to provide valuable assurance and advice. The IIA is dedicated to updating standards and guidance to meet these challenges, ensuring the continued relevance and competence of internal auditors in the digital age."

— David Petrisky, Director,
Professional Standards, The IIA

The technology threat landscape

What you need to know

- **Cybersecurity tops the list.** In terms of the perceived threat level posed to organisations over the next 12 months, cybersecurity stands out as the top-ranked technology risk. Seventy-four percent of respondents consider cybersecurity as a high-risk area, rating it a "4" or "5" on our five-point scale (see Table 1). This percentage climbs even higher, to 82%, among CAEs and IT audit directors (see Figure 2). The good news is that survey respondents indicate their organisations are prepared to handle cybersecurity risks (see Figure 4).
- **Third-party and vendor risks** related to security, reliability and resilience are also a cause for concern (60%), as are risks related to protecting personal data and keeping up with data protection regulations (58%). See Table 1.
- **There are mismatches between threat levels and preparedness.** Our survey results reveal gaps in organisational preparedness in IT talent management, third-party and vendor risk, transformations and system implementations, and data governance (see Figure 4), underscoring an opportunity for action in these areas.
- **AI and ML risk is emerging.** While the short-term perspective indicates a low level of perceived risk (28%) from AI and ML, including generative AI (see Table 1), 54% of our survey participants believe advanced AI systems, including generative AI, present substantial risks in the coming two to three years (see Table 2). The growing utilisation of AI and ML is likely to necessitate a more proactive approach from IT audit teams. This includes, but is not limited to, the establishment of governance and control frameworks and investments in upskilling to gain a better understanding of the unique challenges and risks introduced with AI and ML.
- **The imperative of data governance.** For CAEs and IT audit directors, the accuracy, consistency and reliability of data ranks as the third-highest perceived threat (see Figure 2). Without robust data governance practices in place, organisations may struggle to maintain data quality and integrity, which can hinder decision-making and operational efficiency.

Perceived threat of technology risks in next 12 months (all respondents)

Table 1

Cybersecurity	74%
Third parties/vendors	60%
Data privacy & compliance	58%
Data governance & integrity	55%
Transformations & system implementations	55%
IT talent management	52%
Cloud computing	50%
Technology resiliency	44%
Technical debt & aging infrastructure	43%
Regulatory compliance	41%
Modern software development	36%
IoT	29%
AI & ML (including gen AI)	28%

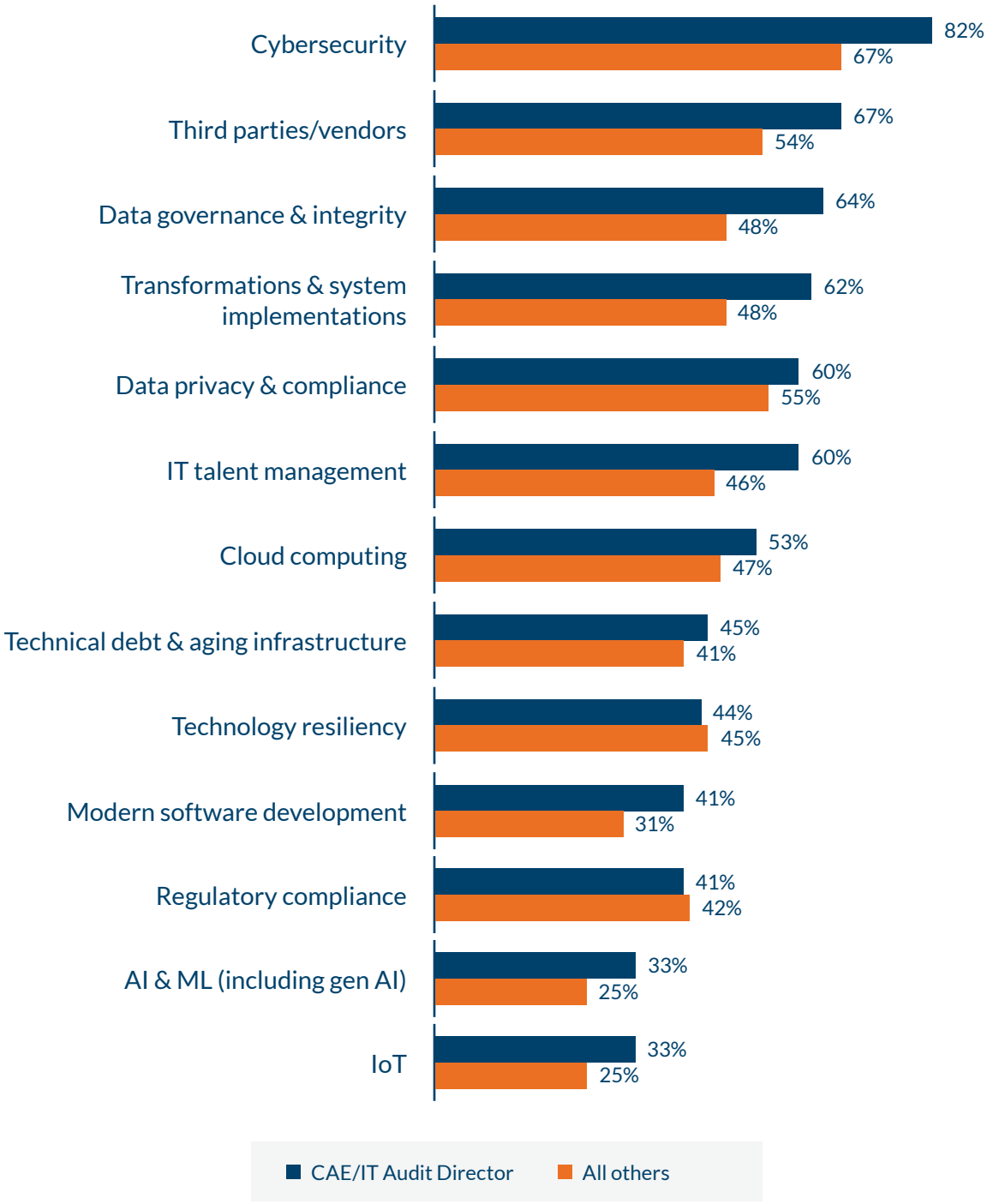
Question: *Please rate the following technology risks in terms of the perceived threat they pose to your organisation over the next 12 months (scale of 1 to 5, where 1 indicates "No threat at all" and 5 indicates "Significant threat" — shown: percentage of responses of "4" or "5"). n=559 — "Other" responses not shown.*

When comparing the responses of CAEs and IT audit directors to those of other professionals within our respondent group (see Figure 2), it becomes evident that CAEs and IT audit directors perceive most of the technology risks as posing a more significant threat to their organisation. The risks with the most substantial gaps include cybersecurity, third parties/vendors, data governance and integrity, transformations and system implementations, and IT talent management.

When evaluating the perceived threat posed by technology risks, particularly in the context of high- and low-frequency technology auditing groups (see Figure 3), it becomes evident that high-frequency auditing organisations view each technology risk as presenting a more substantial threat compared with the views of low-frequency auditing organisations.

Perceived threat of technology risks in next 12 months (CAEs/IT Audit Directors vs. all others)

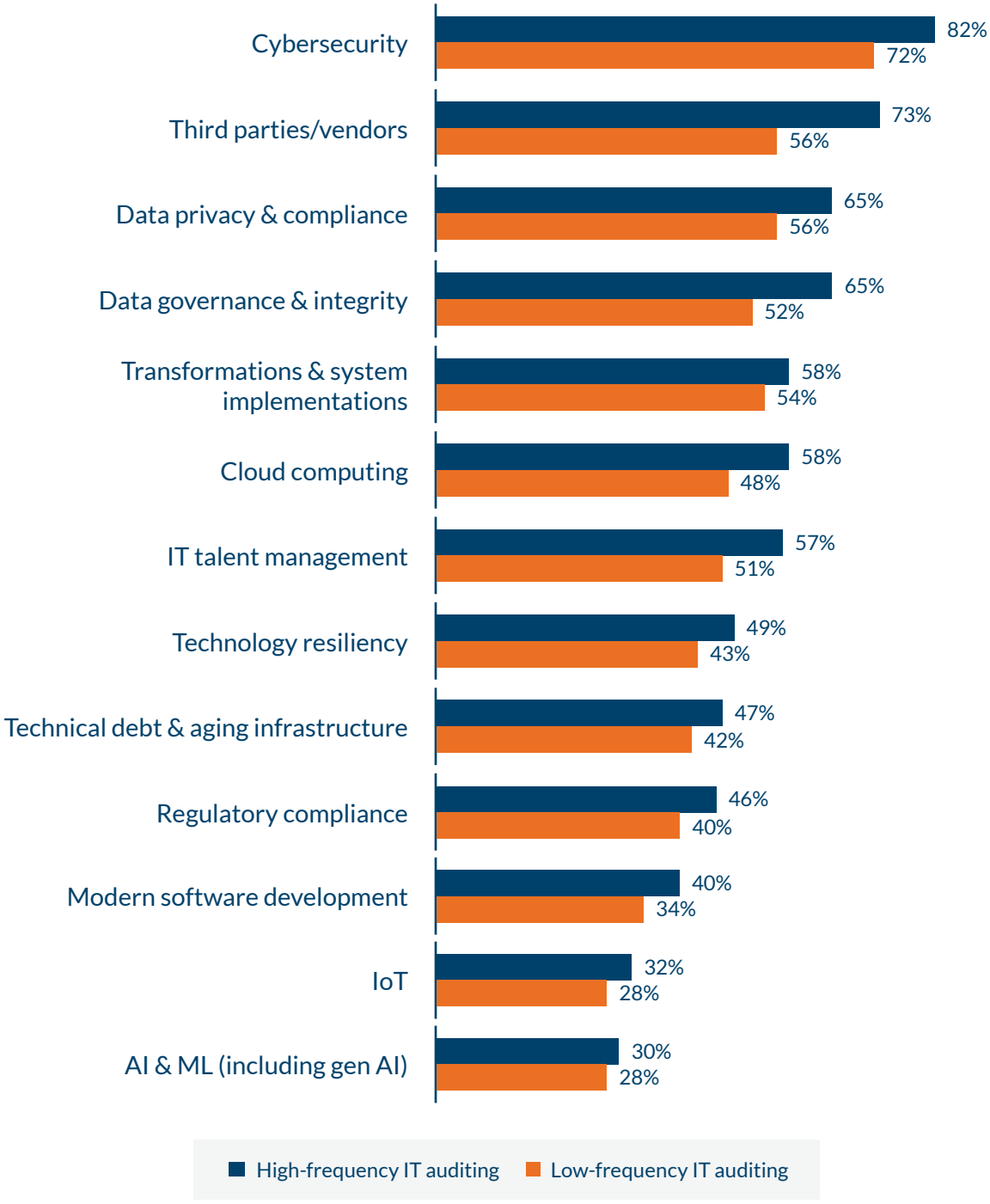
Figure 2



Question: *Please rate the following technology risks in terms of the perceived threat they pose to your organisation over the next 12 months (scale of 1 to 5, where 1 indicates "No threat at all" and 5 indicates "Significant threat" — shown: percentage of responses of "4" or "5"). n=258 (CAE/IT audit director), n=301 (all others) — "Other" responses not shown.*

Perceived threat of technology risks in next 12 months (frequency of IT audits performed)

Figure 3



Question: *Please rate the following technology risks in terms of the perceived threat they pose to your organisation over the next 12 months (scale of 1 to 5, where 1 indicates "No threat at all" and 5 indicates "Significant threat" — shown: percentage of responses of "4" or "5"). n=184 (high-frequency IT auditing), n = 360 (low-frequency IT auditing) — "Other" responses not shown.*

Internal audit opportunities: mapping the risk landscape

The chart below presents an alternative view of the 13 key technology risks assessed in our survey. We have plotted these risks based on the following three variables:

- **Perceived threat level:** The y-axis represents the perceived threat level of each technology risk over the next 12 months, with high threat risks positioned toward the high end of the chart.
- **Organisational preparedness:** The x-axis represents the level of organisational preparedness to handle each technology risk over the next 12 months, with risks for which organisations are most prepared appearing toward the right side of the chart.
- **Technology audit proficiency:** The utilisation of color-coding adds a third dimension, representing technology audit proficiency. We asked survey participants to evaluate how proficient their technology audit team is at effectively assessing each technology risk. Within the chart below, green signifies a high level of proficiency, yellow denotes moderate proficiency and red signifies low proficiency.

Figure 4

About this quadrant

Internal audit departments play a key role in bolstering an organisation's technology risk management capabilities. For areas showcasing high organisational preparedness, internal audits and assurance projects are crucial, affirming that existing processes and controls are both designed and operating effectively. On the flip side, for areas with low organisational preparedness, advisory or consultative projects stand as the bridge, delivering strategic insights and guidance. Prioritising areas with heightened threat levels is wise. In this quadrant, we've categorised the risks into two distinct zones based on our survey findings:

- **Advisory Zone (left side):** Risks residing in this zone highlight gaps in organisational preparedness, indicating a clear need for strategic advice and direction. The higher these risks are plotted, the more pressing the advisory demand becomes due to the rising perceived threat.
- **Assurance Zone (right side):** Risks in this zone indicate areas where organisations feel well-prepared, signalling the importance of routine audits to validate and ensure that control mechanisms are consistently effective.

Note: It is important to understand that actual threat perceptions and readiness levels can vary across organisations. As such, this illustration is rooted primarily in the collective feedback from our survey.

Results depicted in the quadrant are based on the following questions and responses:

Please rate the following technology risks in terms of the perceived threat they pose to your organisation over the next 12 months (scale of 1 to 5, where 1 indicates "No threat at all" and 5 indicates "Significant threat" — shown: percentage of responses of "4" or "5"). n=559.

How prepared is your organisation to handle each of the following technology risks over the next 12 months? (scale of 1 to 5, where 1 indicates "Not at all prepared" and 5 indicates "Extremely prepared" — shown: percentage of responses of "4" or "5"). n=559.

How would you assess the proficiency of your IT audit team at effectively evaluating the following technology risks? (scale of 1 to 5, where 1 indicates "Not at all proficient" and 5 indicates "Extremely proficient" — shown: High IT audit proficiency (green) indicates 50% or more of respondents answered "4" or "5," Moderate IT audit proficiency (yellow) indicates 30%–49.99% of respondents answered "4" or "5," and Low IT audit proficiency (red) indicates less than 30% of respondents answered "4" or "5"). n=559.

Commentary

When comparing perceived threat levels to organisational preparedness for various technology risks, four areas stand out due to the combination of high perceived threat and low organisational preparedness: IT talent management, third parties/vendors, transformations and system implementations, and data governance and integrity. Each represents an area in need of immediate action and strategic attention (see Figure 4).

IT talent management poses a substantial technology risk concern, primarily because of the ongoing demand for qualified individuals with the required skill sets. Amid a long-term talent shortage, those with technology-related skills and talent remain, by far, the most difficult to locate, recruit and retain, especially for technology audit groups. This challenge can rise to the level of a strategic risk in many organisations (see sidebar: "IT talent management risk implications").

The risk related to third parties/vendors is particularly noteworthy as it ranks second overall in terms of perceived threat, suggesting technology audit groups have work to do in improving organisational preparedness around third-party vendor risks (see sidebar: "Challenge your third-party risk management preparedness").

The risks associated with transformations and system implementations can carry substantial consequences, such as operational disruptions, unmet requirements and data loss, especially when not executed properly. Our results indicate that while the perceived threat may not be as high as other risk areas, lack of preparedness in many organisations is a point of concern.

The risks related to data governance and integrity are particularly important, given the dependency on data for guiding business decisions and enabling digital transformations. While this risk may not be at the top of the list of concerns, it certainly poses a challenge in terms of organisational preparedness. Poor data governance can compromise the integrity of AI systems and digital transformations, leading to unreliable results and potential regulatory scrutiny. Effective data governance should not be viewed merely as a compliance exercise but rather as a foundational element that drives competitive advantage.

Level of organisational preparedness to handle technology risks in next 12 months (frequency of IT audits performed)

Figure 5

Question: *How prepared is your organisation to handle each of the following technology risks over the next 12 months (scale of 1 to 5, where 1 indicates "Not at all prepared" and 5 indicates "Extremely prepared" — shown: percentage of responses of "4" or "5"). n=184 (high-frequency IT auditing), n = 360 (low-frequency IT auditing) — "Other" responses not shown.*

Challenge your third-party risk management preparedness

Effective cybersecurity increasingly hinges on the quality of third-party risk management (TPRM) capabilities, so why aren't more organisations prepared to address TPRM-related threats? This is a pressing, yet complicated, question for audit leaders. The lack of TPRM preparedness in organisations today should not be underestimated given research by SecurityScorecard indicates that 98% of organisations maintain a relationship with at least one third party that experienced a cybersecurity breach during the past 24 months.[1]

Our survey indicates organisations are well aware of the potential risks that third parties and vendors pose: Survey respondents rate TPRM as the second most significant perceived threat, behind cybersecurity, over the next 12 months. Further, CAEs and technology audit leaders are more likely to rate TPRM as a perceived threat compared to other survey respondents. So far, so good. Another encouraging indicator: Technology audit leaders and teams give high ratings to their own TPRM proficiency.

The complication arises from the fact that, in the eyes of the technology audit function, organisations are not sufficiently prepared to address TPRM-related threats in the coming year. In fact, in assessing gaps between perceived threat level and organisational preparedness for each technology risk assessed in our study, this TPRM threat level–preparedness difference is the largest such gap in the results.

In terms of remedies, our research suggests it pays to conduct technology audits more frequently and to deploy data analytics when conducting those audits. Technology audit groups that take one or both of these actions are more likely to report that their organisation is prepared to address TPRM threats effectively.

From an enterprisewide perspective, organisations should be prepared to identify, monitor and mitigate third-party (and fourth-party) risks. Based on our experience, third parties tend to have less robust cybersecurity capabilities than their enterprise customers; fourth parties tend to have leaner cybersecurity measures than third parties, and so on. TPRM preparedness requires the collection of actionable information from each third-party risk domain (for example, operational resilience, IT security, privacy, compliance), real-time monitoring, strong key risk indicators, sufficient supporting technology, and streamlined yet highly effective data gathering and assessment processes. These and other areas demand the technology audit team's continued scrutiny and focus on evaluating the organisation's TPRM strategies.

[1] *Close Encounters of the Third (and Fourth) Party Kind*, SecurityScorecard, January 2023: https://securityscorecard.com/research/cyentia-close-encounters-of-the-third-and-fourth-party-kind/.

Trending tech audits

Given the complex landscape of technology risks unveiled through this year's Global Technology Audit Risks Survey, it is important for technology audit leaders to strategise audits that are both current and forward-looking. Within this context, we spotlight prevailing technology audits, classifying them into the following three categories:

- Foundational audits
- Advanced audits
- Emerging audits

While this compilation of technology audits is not exhaustive, it offers a foundation for developing a robust, effective and future-proof IT audit plan.

Foundational audits

Foundational audits are a starting point, especially for organisations with less mature technology audit functions. These audits focus on the core technology risk areas that are essential for every organisation to manage and serve as a foundation for more specialised audits.

- **Cybersecurity program —** Assess the effectiveness of security policies, procedures and controls to safeguard information assets.
- **Data governance and privacy —** Evaluate the framework for data quality, management and protection, including compliance with data privacy regulations.
- **Identity and access management —** Examine controls for ensuring the right individuals have the appropriate access to technology resources.
- **IT asset management —** Evaluate procedures for tracking, valuing and managing IT assets.
- **IT disaster recovery and business continuity —** Assess plans and capabilities for recovering IT systems and maintaining business operations in the event of a disaster.
- **IT governance —** Evaluate the strategic alignment and effectiveness of IT in achieving business objectives.
- **Patch and vulnerability management —** Inspect processes for identifying, reporting and addressing software vulnerabilities.
- **Penetration testing —** Conduct simulated attacks to evaluate the effectiveness of security measures.
- **Third-party risk management —** Assess risks associated with vendors and other third parties.

Advanced audits

Advanced audits dive into rapidly evolving and specialised technology risk areas. These audits provide an opportunity for organisations to conduct in-depth examinations of advanced technologies once the core IT risk areas have undergone comprehensive audits.

- **Cloud security and governance —** Examine controls and compliance in cloud environments.
- **Cyber defence testing and response preparedness —** Evaluate the organisation's readiness to detect, respond to and recover from cyber incidents.
- **DevSecOps —** Assess the integration of security practices within the DevOps process.
- **Microservices architecture —** Audit the security, reliability and performance of microservices-based applications.
- **Privileged access management —** Assess controls over accounts with elevated permissions.
- **Tech architecture and modernisation —** Evaluate the readiness for adopting newer technologies and retiring legacy systems.

Emerging audits

Emerging audits focus on risk areas that represent the cutting edge of technology and are positioned to shape the future landscape of technology risk management. While the types of technologies in this category may not be widespread across all organisations, early audits or diagnostics in these areas can provide a competitive edge by preparing the organisation for potential challenges and opportunities.

- **AI governance and control —** Assess ethical considerations, data usage and decision-making algorithms in AI applications.
- **Automation governance and control —** Audit the governance framework that oversees automated processes and decision-making.
- **Post-quantum cryptography —** Evaluate preparedness for cryptographic challenges posed by quantum computing.

Tailoring technology audit plans to incorporate these three categories of audits aligns the organisation's technology audit strategy with the current and emerging risks identified in our survey. This approach offers a targeted method to mitigate risks and optimise technology's role in achieving business objectives.

Trending tech audits

Through Protiviti's work with hundreds of organisations across all industries, we see the technology audit topics listed below as either foundational, advanced or emerging in internal audit plans being developed for 2024.

Foundational Audits

Focus on the core technology risk areas every organisation needs to manage.

- Cybersecurity Program
- Data Governance & Privacy
- IT Disaster Recovery & Business Continuity
- Identity & Access Management
- IT Asset Management
- IT Governance
- Patch & Vulnerability Management
- Penetration Testing
- Third-Party Risk Management

Advanced Audits

Delve into specific technology risk areas that are maturing and rapidly evolving.

- Cloud Security & Governance
- Cyber Defence Testing & Response Preparedness
- DevSecOps
- Microservices Architecture
- Privileged Access Management
- Tech Architecture & Modernisation

Emerging Audits

Explore risk areas that most represent the future of technology.

- AI Governance & Control
- Automation Governance & Control
- Post-Quantum Cryptography

Risks posed by emerging technologies

We asked respondents to identify the emerging technologies that will pose the most significant risks to their organisations in the next two to three years (see Table 2).

What you need to know

- **Next-gen cyber threats are the most critical emerging risk.** Nearly two out of three respondents (65%) rank next-gen cyber threats as a significant threat, suggesting organisations should prepare to deal with the next generation of cyber threats and cybersecurity challenges.
- **Advanced AI systems are a double-edged sword.** Advanced AI, including generative AI, ranks second, with 54% of respondents highlighting it as an emerging technology risk. Although AI can provide organisations with advantages like automation and enhanced data analysis, its utilisation can also introduce a new level of complexity and risks that organisations need to address and manage proactively.
- **Cloud computing is not just a buzzword.** More than one in three survey respondents (36%) anticipate that cloud computing will pose a threat to organisations in the next two to three years. As more data and services move to the cloud, the imperative to secure them grows.
- **Frequency of audits matters.** The high-frequency IT auditing group views next-gen cyber threats, advanced AI systems and cloud computing as more significant risks compared to the low-frequency IT auditing group (see Figure 7). One possible explanation is that more frequent audits enable the development of a deeper understanding of the complexities these technologies bring. Conversely, those in the low-frequency IT auditing group perceive ESG risks related to technology as greater risks compared with those in the higher frequency IT auditing group. One possible explanation is that organisations performing six or more IT audits in a year may have greater familiarity with the organisation's existing ESG processes, data and metrics.

Emerging technologies expected to pose most significant risks (all respondents)

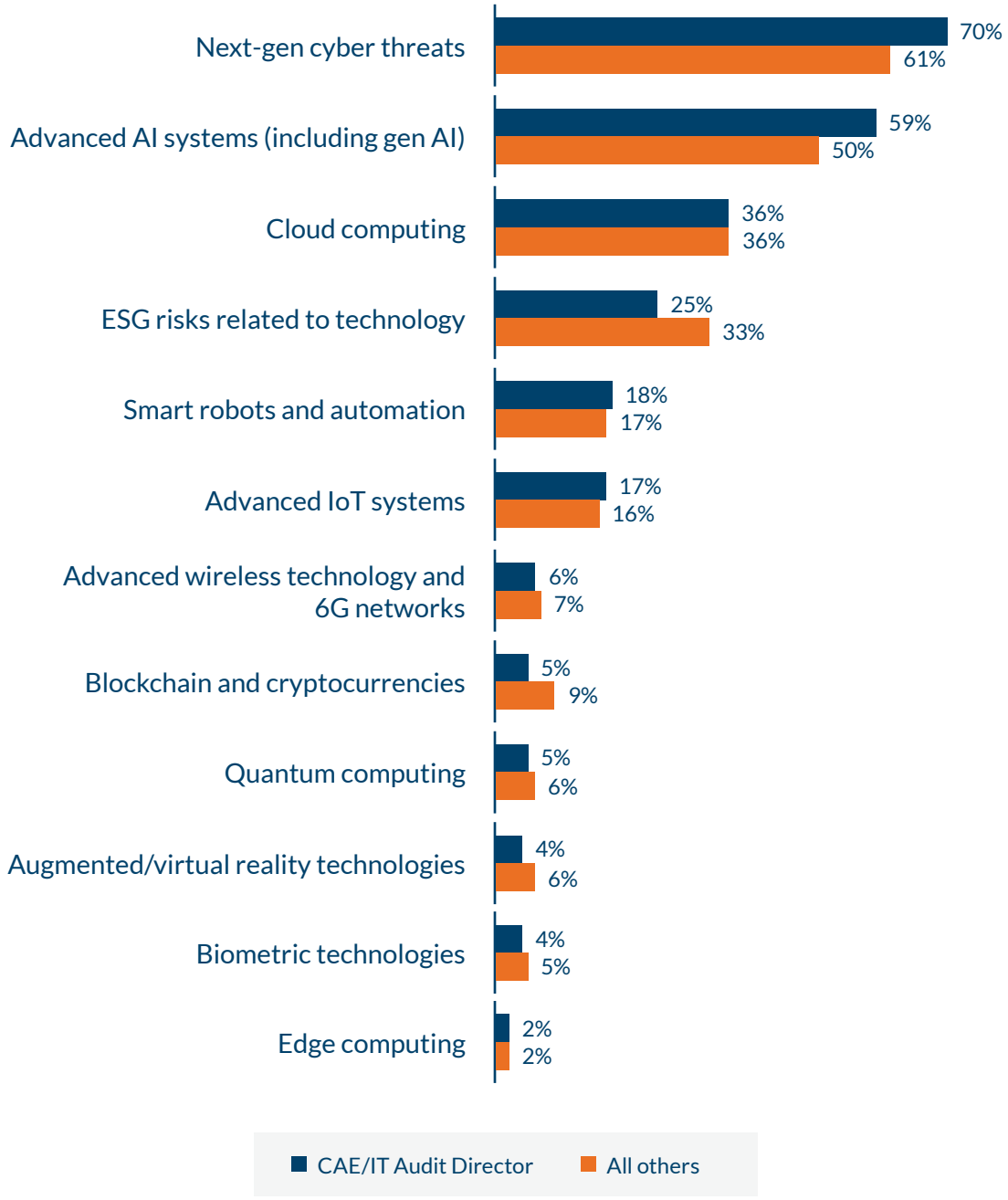
Table 2

Next-gen cyber threats	65%
Advanced AI systems (including gen AI)	54%
Cloud computing	36%
ESG risks related to technology	29%
Smart robots and automation	18%
Advanced IoT systems	17%
Blockchain and cryptocurrencies	7%
Advanced wireless technology and 6G networks	7%
Quantum computing	6%
Augmented/virtual reality technologies	5%
Biometric technologies	4%
Edge computing	2%

Question: *Which of the following emerging technologies, if any, do you anticipate will pose the most significant risks to your organisation in the next 2–3 years? (Up to three responses permitted.) n=559 — "Other" and "None of the above" responses not shown.*

Emerging technologies expected to pose most significant risks (CAEs/IT Audit Directors vs. all others)

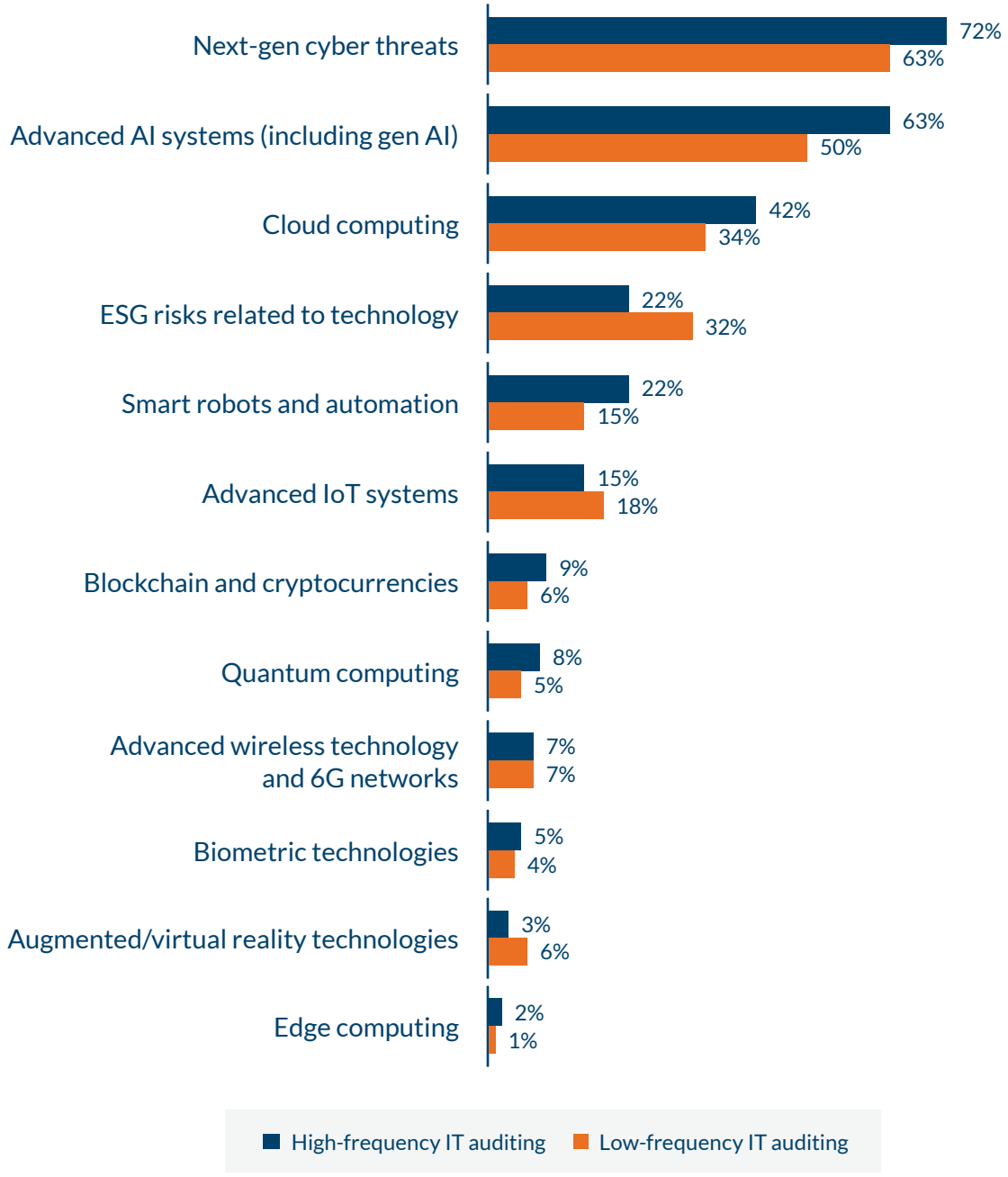
Figure 6



Question: *Which of the following emerging technologies, if any, do you anticipate will pose the most significant risks to your organisation in the next 2–3 years? (Up to three responses permitted.) n=258 (CAE/IT audit director), n =301 (all others) — "Other" and "None of the above" responses not shown.*

Emerging technologies expected to pose most significant risks (frequency of IT audits performed)

Figure 7



Question: *Which of the following emerging technologies, if any, do you anticipate will pose the most significant risks to your organisation in the next 2-3 years? (Up to three responses permitted.) n=184 (high-frequency IT auditing), n = 360 (low-frequency IT auditing) — "Other" and "None of the above" responses not shown.*

Don't sleep on AI risks

Our research reveals that organisations are ill-prepared for AI risks, and technology audit teams lack the proficiency needed to address these threats. This may not be an immediate concern for many organisations considering the use of these technologies remains in the early stages; however, longer term, as the use of AI technologies advances and matures, these deficiencies could pose strategic risks to organisations and create major challenges for technology auditors.

AI adoption, including generative AI and ML technologies, is on the rise. Job listings for AI and ML specialists increased 300% in the past year, while postings for many other IT roles declined.[2] With this rapid adoption of large language models (LLMs) and other types of generative AI across most industries comes greater risk. These risks include "hallucinations" stemming from factual mistakes in source materials, other veracity and authenticity errors, data security, data privacy and confidentiality, ownership/intellectual property (IP), and compliance with applicable laws and regulations.

This context is crucial given technology audit leaders and professionals ranked the organisation's AI and ML preparedness and their technology audit team's level of proficiency to be substantially lower than all other technology risks assessed in our survey. Respondents also perceive AI and ML to be a low threat to organisations over the next 12 months. This is surprising — and tenuous. The growing adoption of generative AI, combined with its warp-speed evolution, is likely to create new types of risks, well beyond the accidental exposure of sensitive IP in open LLMs that larger enterprises already have experienced.

Compared with all other survey respondents, CAEs and technology audit directors are more likely to recognise the nature of AI and ML risks: One in three senior leaders rate these technologies as a perceived threat to the organisation during the next 12 months compared to one-quarter of other respondents. That's a good start. Our view is that these executives should lead the way in improving AI risk management preparedness and proficiency sooner rather than later.

[2] "The $900,000 AI Job Is Here," Chip Cutter, *The Wall Street Journal*, Aug. 14, 2023: www.wsj.com/articles/the-900-000-ai-job-is-here-230fc3cb.

Technology tools in use and adoption barriers

We asked respondents to identify the tools, technologies and delivery methods that are currently used to support their IT audit department.

What you need to know

- **Collaboration tools lead the pack.** Collaboration tools are currently being used by 68% of respondents, underscoring the importance of team coordination in effective risk management (see Figure 8).
- **Audit frequency drives tech enablement.** High-frequency auditing organisations report higher use of tools, technologies and delivery methods to support their technology audit departments (see Figure 10).
- **Budget constraints stifle adoption.** A majority of respondents (52%) report a lack of budget as a barrier to adopting new tools and technologies to support their technology audit function (see Figure 11).
- **Data analytics elevates proficiency.** Technology audit functions that employ data analytics tools consistently score higher in their proficiency to evaluate technology risks (see Figure 9). The integration of data analytics into the audit process is thus not merely a nice-to-have but a strategic imperative.
- **AI and ML lag behind.** Despite the increased interest in AI and ML, only 12% of respondents indicate that their organisations have adopted AI and ML technologies within their audit functions (see Figure 8). While there are multiple potential factors contributing to this low adoption rate, a couple of possibilities include a lack of governance and controls, as well as a lack of proficiency in implementation.

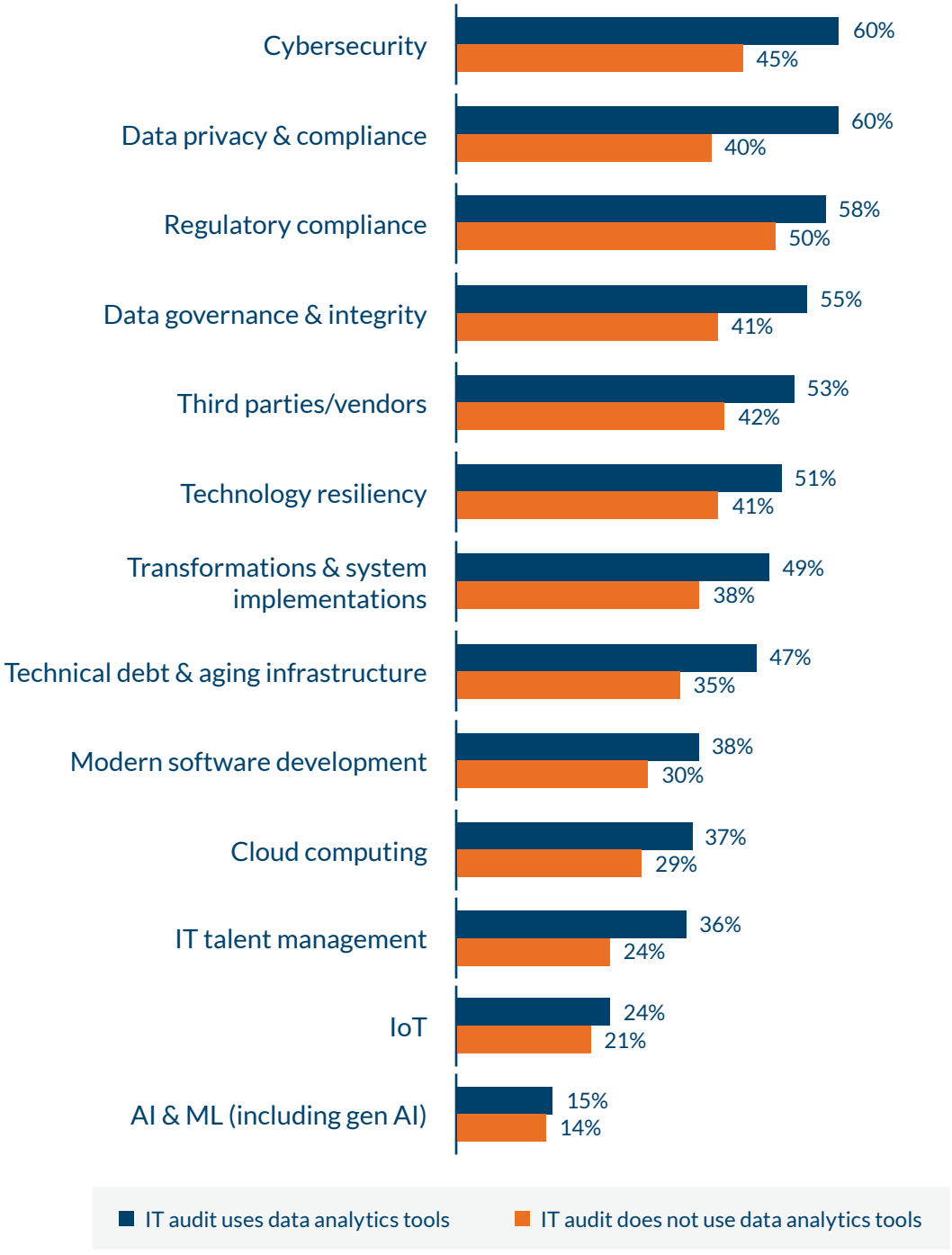
Tools/technologies/delivery methods used to support the IT audit department (all respondents)

Figure 8

Question: *Which of the following tools, technologies or delivery methods, if any, are currently used to support your IT audit department? (Multiple responses permitted.) n=559 — "Other" and "None of the above" responses not shown.*

Proficiency of IT audit team to evaluate technology risks (based on use of data analytics tools — see Figure 8)

Figure 9



Question: *How would you assess the proficiency of your IT audit team at effectively evaluating the following technology risks? (scale of 1 to 5, where 1 indicates "Not at all proficient" and 5 indicates "Extremely proficient" — shown: percentage of responses of "4" or "5"). n=316 (IT audit uses data analytics tools), n = 243 (IT audit does not use data analytics tools) — "Other" responses not shown.*

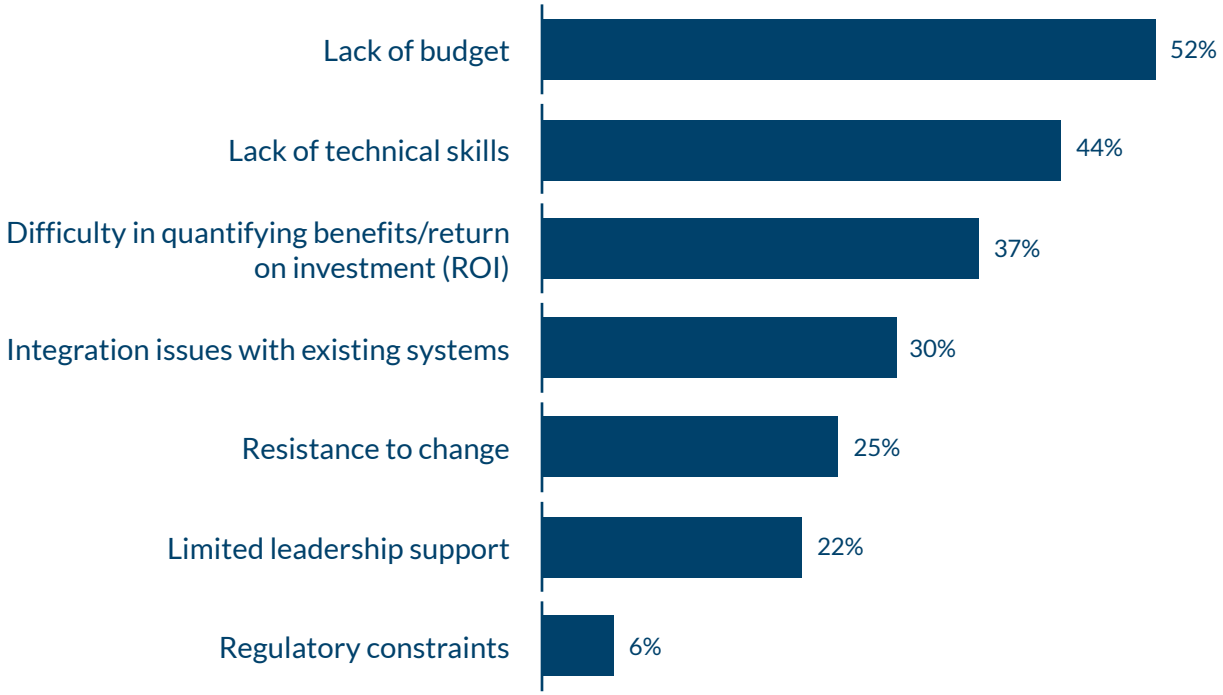
Tools/technologies/delivery methods used to support the IT audit department (frequency of IT audits performed)

Figure 10

Question: *Which of the following tools, technologies or delivery methods, if any, are currently used to support your IT audit department? (Multiple responses permitted.) n=184 (high-frequency IT auditing), n = 360 (low-frequency IT auditing) — "Other" and "None of the above" responses not shown.*

Barriers to adopting IT audit tools and technologies (all respondents)

Figure 11



Question: *Which of the following barriers, if any, has your IT audit department encountered in adopting these tools and technologies? (Up to three responses permitted.) n=559 — "Other" and "None of the above" responses not shown.*

Managing technology risks and identifying talent and support needs

We asked respondents to identify the actions their technology audit department is taking to address both current and emerging technology risks, as well as to specify the resources or support they believe their technology audit department requires for more effective management of these risks.

What you need to know

- **Talent management and collaboration are key.** To manage current and emerging technology risks, IT audit departments are focusing on: upskilling/reskilling staff, strengthening collaboration between IT audit and IT/cybersecurity teams, and collaborating with external partners (see Figure 12). The focus on upskilling and reskilling staff underscores the importance of addressing IT talent management challenges proactively. As noted earlier, IT talent management is positioned in our risk quadrant (which depicts a view of technology risks based on three dimensions: perceived threat level, organisational preparedness and technology audit proficiency — see Figure 4) as presenting a higher level of threat combined with a lower level of preparedness. Further, survey respondents indicate their technology audit teams are moderately proficient at effectively evaluating such technology risk.
- **Organisations need better training.** Close to half of respondents (45%) believe their technology audit department needs enhanced training programs for staff to manage both current and emerging technology risks more effectively (see Figure 14). The need for such training is higher (54%) within the high-frequency auditing group, compared to 41% in the low-frequency auditing group (see Figure 15).
- **Addressing talent needs is the priority for improved technology risk management.** Talent- and skills-related actions stand out as most frequently pursued to manage current and emerging technology risks (see Figure 14). In contrast, IT talent management poses a substantial technology risk issue, with a lack of corresponding organisational readiness and technology audit group proficiency (see Figure 4). This underscores the importance of addressing IT talent management challenges proactively (see sidebar: "IT talent management risk implications").

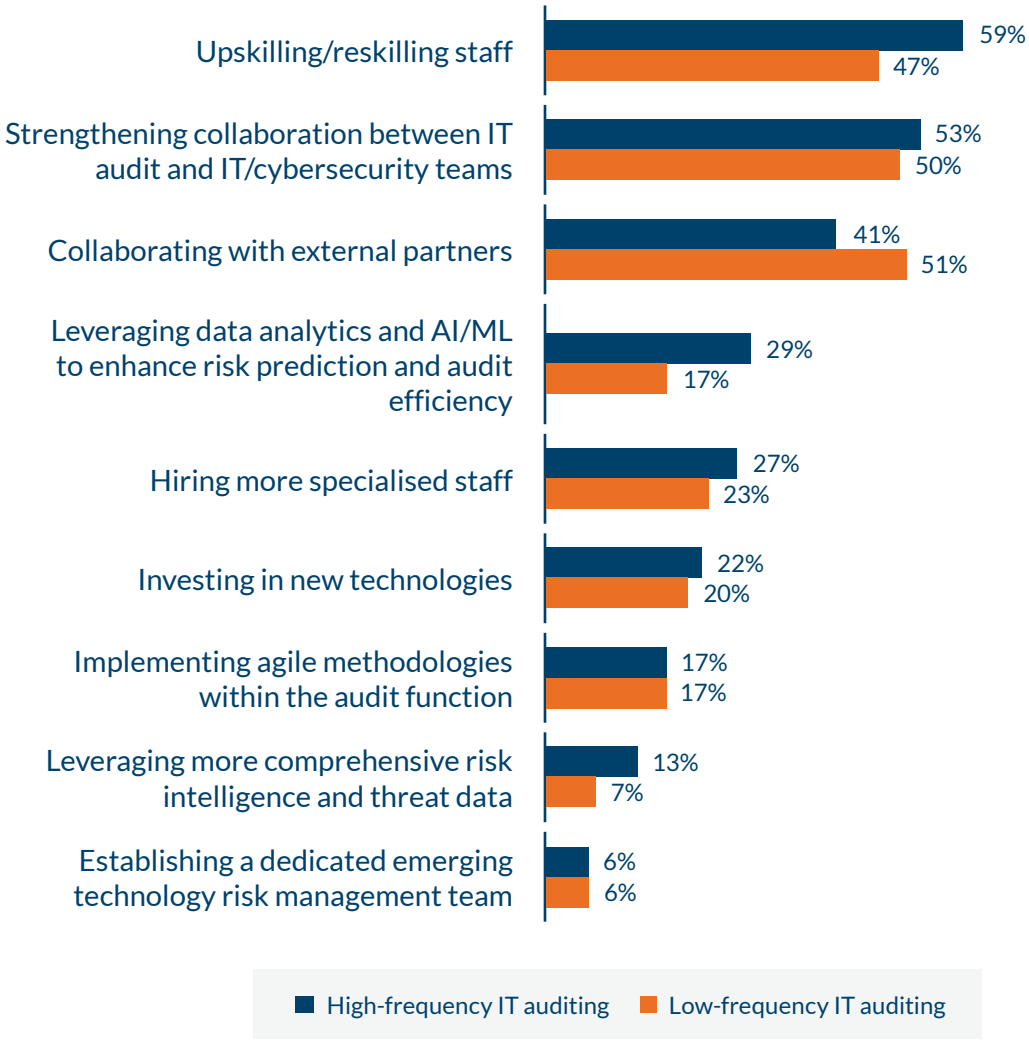
Actions taken to manage current and emerging technology risks (all respondents)

Figure 12

Question: *Which of the following actions, if any, is your IT audit department taking to manage both current and emerging technology risks? (Up to three responses permitted.) n=559 — "Other" and "None of the above" responses not shown.*

Actions taken to manage current and emerging technology risks (frequency of IT audits performed)

Figure 13



Question: *Which of the following actions, if any, is your IT audit department taking to manage both current and emerging technology risks? (Up to three responses permitted.) n=184 (high-frequency IT auditing), n = 360 (low-frequency IT auditing) — "Other" and "None of the above" responses not shown*

Resources/support needed to manage current and emerging technology risks (all respondents)

Figure 14

Question: *What resources or support, if any, do you believe your IT audit department needs to more effectively manage both current and emerging technology risks? (Up to three responses permitted.) n=559 — "Other" and "None of the above" responses not shown.*

Resources/support needed to manage current and emerging technology risks (frequency of IT audits performed)

Figure 15

Question: *What resources or support, if any, do you believe your IT audit department needs to more effectively manage both current and emerging technology risks? (Up to three responses permitted.) n=184 (high-frequency IT auditing), n = 360 (low-frequency IT auditing) — "Other" and "None of the above" responses not shown.*

IT talent management risk implications

Our survey results show that improvements in organisational preparedness and technology audit proficiency related to IT talent management are widely needed. How well auditing teams address long-term IT talent management risks can have implications on other technology risks as well as the associated risk management capabilities.

The technology audit team's ability to address significant risks, such as cybersecurity, TPRM, and data privacy and compliance, among others, depends on the supply of high-quality IT talent and the audit function's ability to recruit, retain and develop skilled technology auditors. These activities have grown increasingly difficult to execute in the face of a systemic talent shortage that is especially acute among highly technical professions (e.g., auditing and accounting) and roles that demand IT-related skills and experience (particularly related to advanced technologies). Not surprisingly in this environment, according to our results, CAEs and technology audit leaders rate IT talent management as more of a perceived threat over the next 12 months than other respondents (see Figure 2).

In our view, to address IT talent management challenges effectively, internal audit groups need a two-pronged response. First, they need to understand and adapt to an emerging employee-employer compact as traditional hiring approaches give way to entirely new talent strategies. Second, audit leaders should understand and deploy next-generation talent management approaches related to skills sourcing, job and workforce redesign, talent analytics, recruiting, retention, leadership development, and succession planning.[3]

[3] For more information, read Protiviti's series on workforce management and talent planning, available at www.protiviti.com/gl-en/bulletin.

In closing — our strategic outlook

The key takeaway is clear. Now is the time for technology audit groups to evolve their practices to better manage an increasingly complex landscape of technology risks.

Our survey results reveal a dichotomy in technology risk management capabilities. While organisations appear well-equipped to manage traditional compliance-related risks, they fall short in preparedness and proficiency levels for emerging technology risks like AI, ML, third-party vendor management and IT talent management.

This imbalance calls for immediate action. Technology audit groups must apply the same disciplines, processes and rigour used in compliance audits to these emerging areas of technology risk.

Demographics

The following tables reflect the demographics of the survey participants.

Position

n = 559

Chief Audit Executive (or equivalent)	33%
IT Audit Director	13%
Audit Director	9%
IT Audit Manager	14%
Audit Manager	10%
IT Audit Staff	4%
Audit Staff	4%
IT Risk/Control Manager	2%
IT Risk/Control Specialist	2%
IT Risk/Control Executive	1%
IT Executive	1%
IT Risk/Control Director	1%
IT Manager	1%
Other	5%

Industry

n = 559

Financial Services — Banking	13%
Technology (Software, High-Tech, Electronics)	9%
Manufacturing (other than Technology)	8%
Financial Services — Other	6%
Insurance (other than Healthcare Payer)	6%
Government	4%
Healthcare Provider	4%
Transportation and Logistics	4%
Financial Services — Asset Management	3%
Power and Utilities	3%
Retail	3%
Higher Education	3%
Telecommunications and Data Infrastructure	3%
Professional Services	3%
Consumer Packaged Goods	2%
Healthcare Payer	2%
Oil and Gas	2%
Real Estate	2%
Automotive	2%
Hospitality, Leisure and Travel	2%
Financial Services — Broker-Dealer	1%
Financial Services — Payments	1%
Media	1%
Pharmaceuticals and Life Sciences	1%
Airlines	1%
Construction	1%
Wholesale and Distribution	1%
Mining	1%
Not-for-profit	1%
Agriculture, Forestry and Fishing	1%
Chemicals	1%
Other	5%

Organisation type

n = 559

Publicly traded	44%
Privately held	34%
Government	9%
Not-for-profit	8%
Other	5%

Size of organisation (other than financial services) — by gross annual revenue in U.S. dollars

n = 406

$20 billion or more	10%
$10 billion - $19.99 billion	10%
$5 billion - $9.99 billion	10%
$1 billion - $4.99 billion	28%
$500 million - $999.99 million	11%
$100 million - $499.99 million	9%
Less than $100 million	8%
Unsure	14%

Size of organisation (financial services organisations) — by annual assets under management in U.S. dollars

n = 130

$250 billion or more	14%
$50 billion - $249.99 billion	14%
$25 billion - $49.99 billion	10%
$10 billion - $24.99 billion	12%
$5 billion - $9.99 billion	8%
$1 billion - $4.99 billion	15%
Less than $1 billion	12%
Unsure	15%

Size of government agency's annual budget — in U.S. dollars

n = 23

$50 billion or more	0%
$10 billion - $49.99 billion	0%
$5 billion - $9.99 billion	17%
$1 billion - $4.99 billion	13%
$500 million - $999.99 million	4%
$100 million - $499.99 million	22%
Less than $100 million	31%
Unsure	13%

Audit department headcount

n = 559

0-4	23%
5-9	24%
10-19	20%
20-29	9%
30+	24%

Total number of full-time technology auditors

n = 559

0	13%
1	24%
2	16%
3	10%
4	7%
5	7%
6-10	11%
11+	12%

Organisation headquarters

n = 559

North America	47%
Europe	24%
Asia-Pacific	21%
Africa	4%
Middle East	4%

Technology audit department headquarters

n = 559

North America	47%
Europe	24%
Asia-Pacific	22%
Middle East	4%
Africa	2%
Other	1%

About The IIA

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 235,000 global members and has awarded more than 190,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognised throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

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 our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®

www.protiviti.com

The Institute of Internal Auditors

www.theiia.org