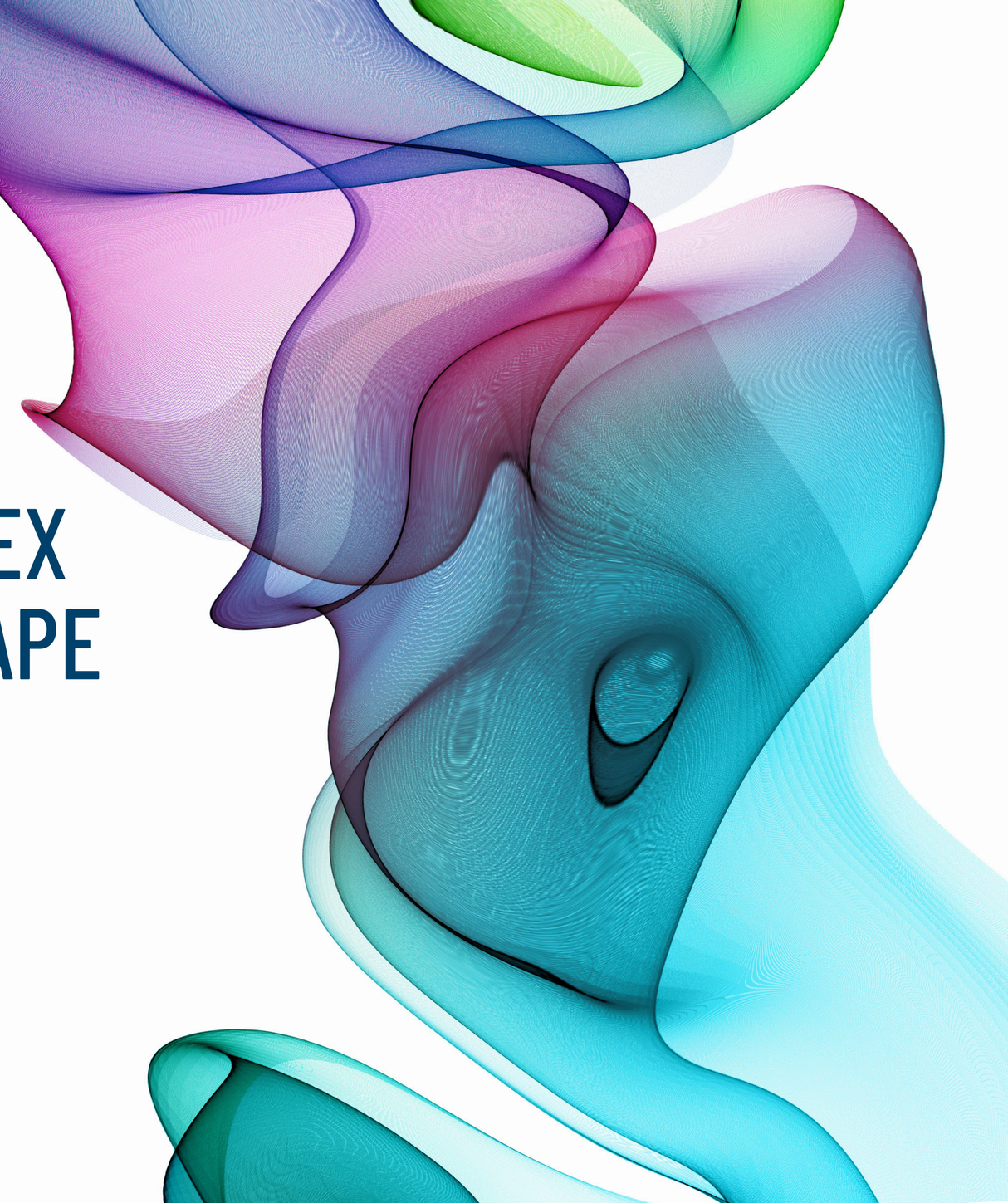
protiviti®
Global Business Consulting

The Institute of
Internal Auditors

FROM AI TO CYBER — DECONSTRUCTING A COMPLEX TECHNOLOGY RISK LANDSCAPE

Assessing the results of the 12th Annual Global Internal Audit Perspectives on Top Technology Risks Survey from Protiviti and The Institute of Internal Auditors



GLOBAL INTERNAL AUDIT

TABLE OF CONTENTS

01

Executive summary and key findings

Cybersecurity. Data privacy and governance. Artificial intelligence (AI). Third-party risk.

At first glance, the results of this year's **Global Internal Audit Perspectives on Top Technology Risks Survey** paint a familiar picture of the primary technology threats faced by organizations worldwide and their readiness to tackle them. However, a deeper look reveals nuanced layers that depict today's and tomorrow's challenges in different hues and dimensions. More important, the findings highlight the strategies and tools that are proving most effective for technology auditors to address these challenges.

The results not only reinforce some trends from prior years, but also reveal emerging risk trends that technology auditors must anticipate to remain relevant. There is greater interest in new approaches to address the changing risk landscape, and there is an elevated level of maturity in some organizations, which signals what is to come for the technology audit profession.

As noted in the key findings, cybersecurity is viewed as the most significant technology threat. Data breaches top the list of perceived cybersecurity-related threats, largely due to increased concerns around ransomware attacks. In addition, our research reveals the greatest perceived risks associated with AI are, by a considerable margin, security and privacy issues, underscoring the dominance of cybersecurity as a critical challenge.

Beyond cyber issues, AI is rapidly becoming a critical area for technology auditors. Despite AI's growing influence, proficiency in AI-related auditing remains low, highlighting the urgent need for audit groups to bolster their knowledge of AI risks, including ethical, operational and reputational challenges.

Factors such as audit frequency stand out in the survey results. Internal audit functions that perform six or more technology audits annually, referred to as *high-frequency IT auditing groups*, perceive the threat landscape and their overall preparedness in a much different light — a topic we explore further in our analysis.

Perceived high threat levels for cybersecurity over next 12 months*

68% All organizations

76% Organizations employing AI tools in technology audits

76% Organizations employing cybersecurity tools in technology audits

79% Organizations that perform six or more technology audits annually

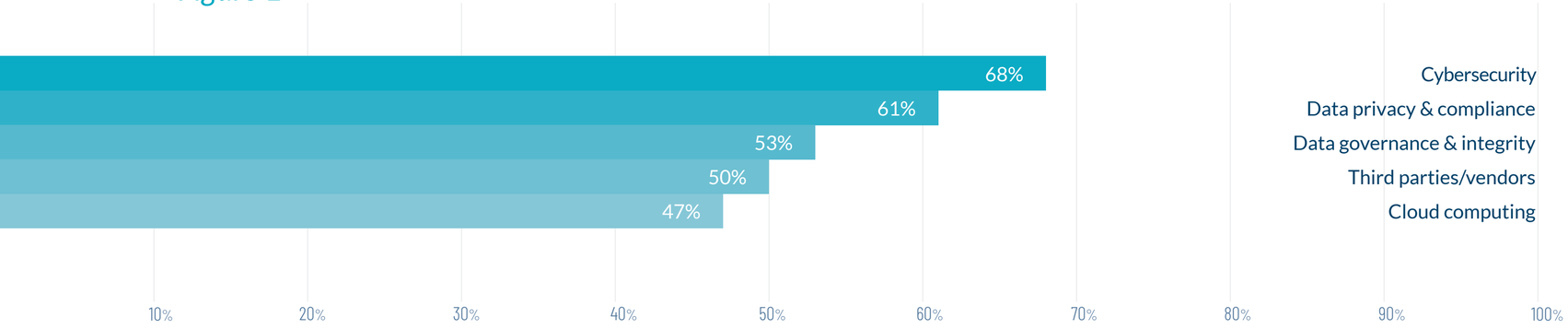
* Percentages reflect the number of respondents who rated the threat a 4 or 5 on a 5-point scale, where 1 indicates "No threat at all" and 5 indicates "Significant threat."

Audit frequency is among several important indicators for technology audit functions as they navigate a dynamic business landscape that is being shaped continually by exponential growth in technologies like generative AI and the concurrent emergence of new security, privacy and data-related challenges.

In the following pages, we present the key findings from the survey, the complete set of risks and definitions, and the analysis supporting our conclusions. Our call to action (see page 28) summarizes the key activities audit groups should undertake to ensure their technology audit functions continue to deliver value and remain relevant to their organizations. Lastly, the Appendix contains a comprehensive overview of the global survey results.

Top 5 technology risks*

Figure 1



*Percentages reflect the number of respondents who rated the threat a 4 or 5 on a 5-point scale, where 1 indicates "No threat at all" and 5 indicates "Significant threat."

Global Internal Audit Standards™

In January 2024, The Institute of Internal Auditors published an updated version of the Global Internal Audit Standards™ ("the Standards"). These standards are a mandatory component of the International Professional Practices Framework (IPPF), which facilitates the consistent development, interpretation, and application of internal auditing knowledge, thereby enhancing the profession. Applicable standards are referenced throughout this publication, with further information available via The IIA's website: **www.theiiia.org/NewStandards**.

Our key findings

Cybersecurity is the top technology threat — Not only do cyber concerns stand out as the top threat, but these concerns are even greater among organizations conducting technology audits more frequently, as well as among those using cybersecurity and AI-based tools to support the technology audit department. These more mature organizations also expressed the highest level of preparedness to handle this risk (Standard 9.1 Understanding Governance, Risk Management, and Control Processes).

AI is beginning to influence technology auditing — While AI is not viewed as a significant short-term technology concern, most respondents (59%) view advanced AI systems as posing significant risks to their organizations in the next two to three years. Further, the use of AI-based tools in technology auditing is associated with elevated concerns about various threats, including cybersecurity and data privacy, and also drives higher levels of perceived organizational preparedness to handle such threats (Standard 10.3 Technology Resources).

Data concerns are prevalent — Data privacy and compliance as well as data governance and integrity rank among the top technology risks organizations face, and 52% view data breaches and leaks of sensitive information as posing the greatest cybersecurity-related threats.

Higher frequency of technology audits drives better performance — Conducting more technology audits annually (for purposes of analyzing this survey's results, defined as six or more — see page 8) drives a clearer understanding of the threat landscape and contributes to improved organizational preparedness and technology audit proficiency to handle these threats. Conversely, organizations with lower audit frequency may face blind spots in their risk management efforts, underscoring the importance of regular and thorough auditing (Standards 9.4 Internal Audit Plan; 13.2 Engagement Risk Assessment).

About our survey

Protiviti partnered with The Institute of Internal Auditors (The IIA) to conduct its 12th annual Global Internal Audit Perspectives on Top Technology Risks Survey in the second quarter of 2024. The objective of this annual survey is to explore the top technology risks organizations face, as perceived by technology audit leaders and professionals. Additionally, it explores the practices, processes and tools employed to help enterprises identify, assess, manage and mitigate these risks. A total of 1,246 executives and professionals, including chief audit executives (CAEs) and information technology (IT) audit directors, completed the survey this year.

Definitions of survey-assessed technology risks

In this year's survey, we assessed 13 technology risks that organizations 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 unauthorized access, disruption or destruction of information, systems or networks.

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

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

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

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

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

Software development — Risks associated with modern software development and deployment, such as DevOps, continuous integration and continuous delivery (CI\CD), and containerization.

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

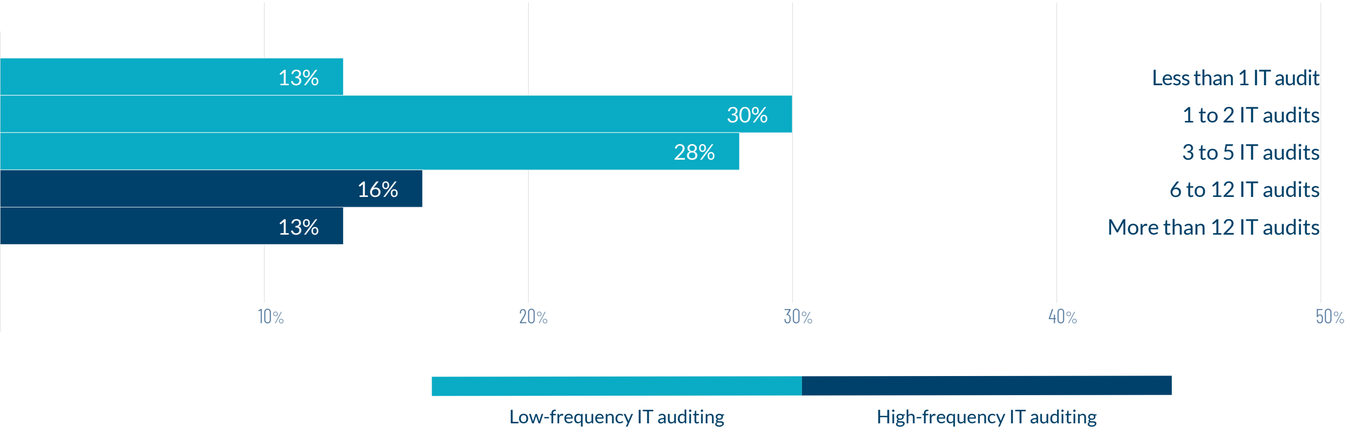
Similar to the analysis conducted in the 2023 study, a metric examined in this year's survey is how often organizations conduct technology audits. The survey responses were categorized into two distinct groups:

High-frequency IT auditing — Organizations that conduct six or more technology audits per year

Low-frequency IT auditing — Organizations that conduct five or fewer technology audits per year

These high- and low-frequency IT auditing groups are referenced throughout the report. As illustrated in Figure 2 below, the majority (71%) of respondents indicate that their organizations perform five or fewer technology audits per year.

Figure 2



"Unsure" responses not shown.

59%

of organizations anticipate advanced AI systems (including generative AI) will pose significant risks in the next two to three years.

02

Top technology threats, organizational preparedness and IT audit proficiency

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

Table 1

	2024	2023	YOY trends
Cybersecurity	68%	74%	↓
Data privacy & compliance	61%	58%	↑
Data governance & integrity	53%	55%	↓
Third parties/vendors	50%	60%	↓
Cloud computing	47%	50%	↓
Regulatory compliance	44%	41%	↑
IT talent management	43%	52%	↓
Transformations & system implementations	43%	55%	↓
Technology resiliency	36%	44%	↓
Technical debt & aging infrastructure	33%	43%	↓
Software development	29%	36%	↓
AI & machine learning (including generative AI)	28%	28%	↔
IoT	22%	29%	↓

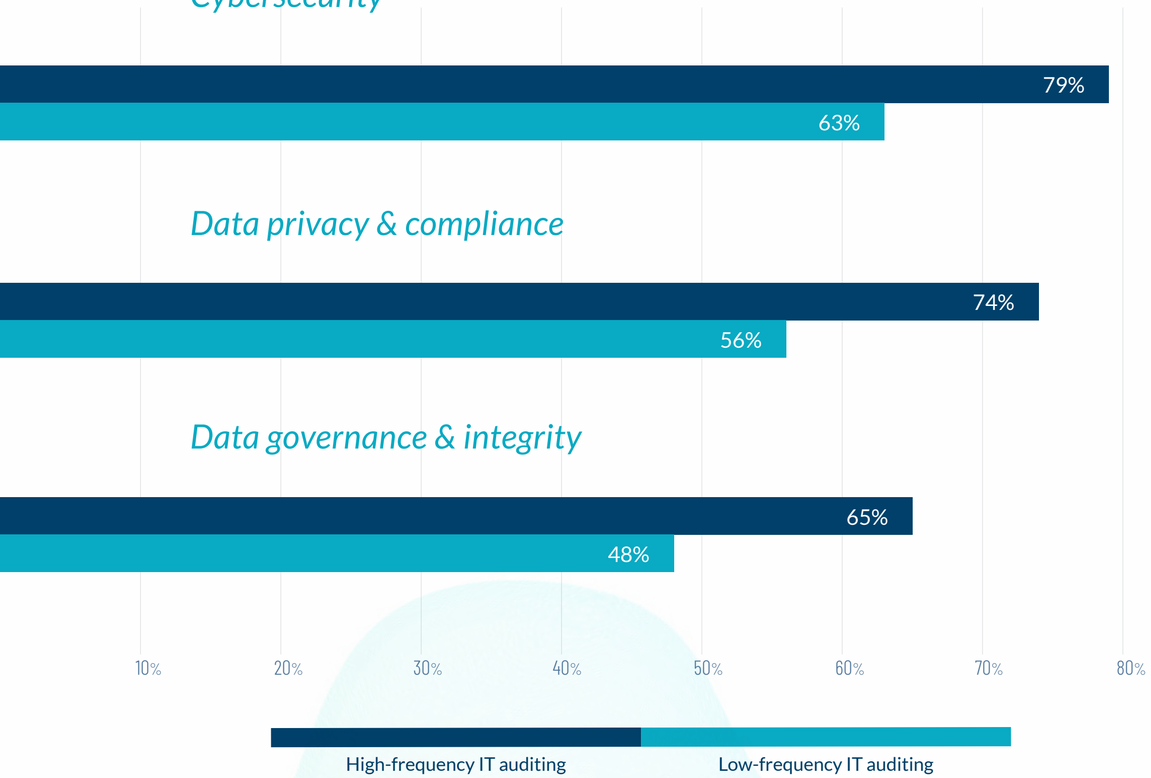
*Percentages reflect the number of respondents who rated the threat a 4 or 5 on a 5-point scale, where 1 indicates "No threat at all" and 5 indicates "Significant threat."

Cyber and data stand out: Technology auditors should be well-acquainted with the top-rated technology risks in this year's survey, which include cybersecurity, data privacy and governance, third parties, and cloud computing.

Threat levels are down, preparedness levels are up … for some: The year-over-year trend indicates a moderate decrease in perceived technology-related threats and an increase in preparedness among organizations to manage these risks, with just two areas — data privacy and compliance, and regulatory compliance — showing year-over-year increases in perceived threat levels. Given the broad attention on technology-related threats over the past year, many companies likely have matured their risk management programs. This includes enhancing cybersecurity measures, resulting in perceptions of decreasing threat levels and increasing organizational preparedness. Additionally, more organizations are adopting advanced technologies to support threat detection response (see Figure 16).

Perceived threat of technology risks in next 12 months — perspectives among high-frequency IT auditing groups*

Figure 3



*Percentages reflect the number of respondents who rated the threat a 4 or 5 on a 5-point scale, where 1 indicates "No threat at all" and 5 indicates "Significant threat."

Going deeper: However, the perceived threat levels of technology risks over the next 12 months, as shown in Table 1, do not provide a complete picture. Assessing the results among specific groups of respondents, such as those that use cybersecurity detection or AI-based tools, as well as organizations that represent high-frequency IT audit functions, reveals interesting variations. These groups often perceive a broader and more significant threat landscape while viewing their organizations as better prepared to mitigate these risks. This suggests less advanced audit teams might perceive a narrower or more limited set of technology-related risks.

Third-party gaps: Interestingly, third-party and vendor risk represents a significant gap for technology audit teams, as perceived threat levels are relatively high while the level of proficiency in the IT audit team to evaluate this issue are notably lower. Also, there is a significant year-over-year drop in technology audit proficiency to evaluate this risk (see Table 3).

Commentary

Our findings reveal several key differentiators for IT audit functions to improve performance and deliver greater value to the enterprise. As observed in last year's study, the frequency of technology audits performed annually reveals significant differences in how IT audit leaders and teams perceive threats and assess the organization's preparedness to manage them. This is particularly evident in areas such as cybersecurity, regulatory compliance, data privacy and compliance, and data governance and integrity. These differences suggest that high-frequency IT auditing groups may have a better understanding of these risks and the threats they pose to the organization.

Much of this is understandable. Internal audit functions that perform technology audits more frequently are naturally expected to have more concerns about the technology risk landscape. However, these differences are not visible across all technology risks.

As noted earlier, two technology risks have increased year over year in terms of perceived threat to the organization: data privacy and compliance, and regulatory compliance (see Table 1). The contributing factors to this uptick likely include evolving regulations and the increasing complexity of data governance. Business leaders need to upgrade their data privacy and governance frameworks continuously to ensure compliance remains a top priority.

Additionally, cybersecurity remains a significant technology threat, driven in great part by elevated concerns about ransomware attacks. However, the perceived level of preparedness for cybersecurity is rising, with 63% of respondents indicating their organizations are well-prepared to handle cyber threats (see Table 2). This progress reflects not only the growing adoption of advanced cybersecurity tools — such as vulnerability scanners and threat intelligence platforms — but also the increasing prioritization of cybersecurity at the board level. As cybersecurity becomes a strategic concern for leadership, organizations are dedicating more resources and attention to enhancing their defenses, resulting in stronger overall security postures.

Further, notable differences are observed among organizations that use cybersecurity tools (or assess the outputs of their use by the business), as well as AI and machine learning tools, to support their IT auditing activities. This suggests that these tools are valuable assets in helping IT audit teams identify specific technology threats and understand the organization's level of preparedness to manage them. By leveraging these tools, IT audit teams can scan entire networks and identify gaps in near real-time. As a result, they become more security conscious and aware, enabling them to develop a better appreciation of all threats. However, it is important for technology audit teams to partner with the IT organization to understand how these tools are being used throughout the enterprise and to optimize ways for the internal audit function to leverage them (Standards 13.4 Evaluation Criteria; 13.5 Engagement Resources,13.6 Work Program).

These findings certainly raise several important questions. For example, what might organizations that are not utilizing cybersecurity or AI tools, or conducting technology audits frequently, be missing in their technology audits and risk coverage?

In regard to third-party risk management, the significant gap between perceived threat level and the organization's preparedness to handle this risk suggests companies recognize third-party and vendor risks as a major threat but believe they are underprepared to manage them effectively. This could be due to the complexities involved in managing third-party relationships and the potential cascading effects of vendor vulnerabilities on the organization. It's also possible that, at least in some organizations, there is no clearly defined owner of third-party risk management.

"These are remarkably dynamic times for organizations, not only due to rapidly changing market conditions but also resulting from ongoing technology transformation, led by the rapid rise of generative AI. Internal audit teams need to keep pace with the changes their organizations continue to undergo. More importantly, they need to embrace the use of emerging technologies like generative AI and advanced analytics in their own internal audit practices as they help to identify and address the most critical technology risks their organizations face."

– **Angelo Poulikakos**
Managing Director, Global Leader,
Technology Audit and Advisory, Protiviti

Perceived level of organizational preparedness to handle technology risks in next 12 months (all respondents)*

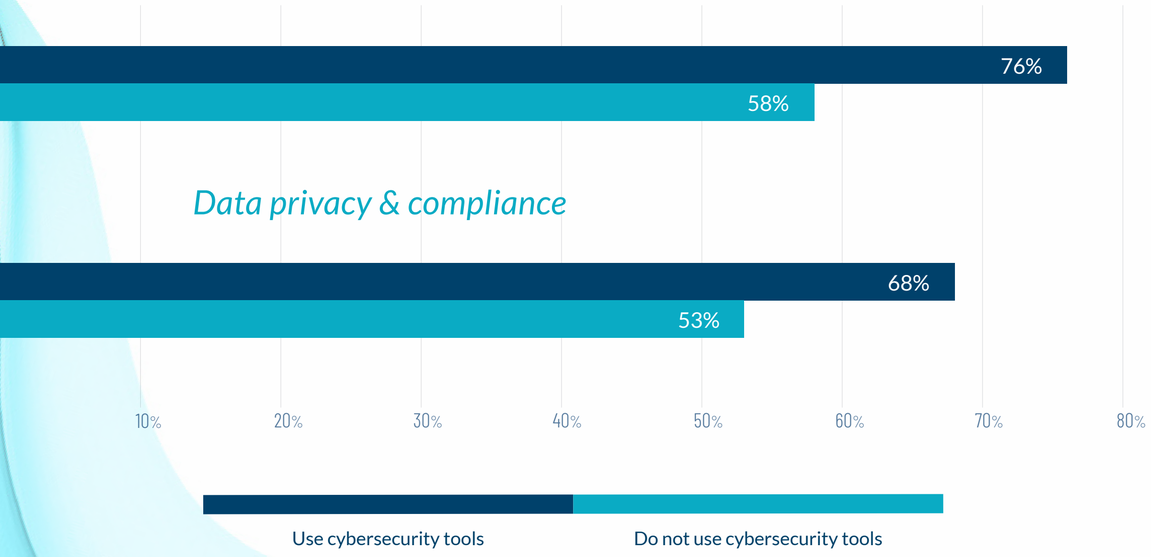
Table 2

	2024	2023	YOY trends
Cybersecurity	63%	55%	↑
Regulatory compliance	57%	53%	↑
Data privacy & compliance	55%	45%	↑
Cloud computing	47%	42%	↑
Data governance & integrity	47%	35%	↑
IT talent management	44%	25%	↑
Transformations & system implementations	39%	36%	↑
Software development	38%	35%	↑
Technology resiliency	37%	45%	↓
Third parties/vendors	36%	30%	↑
Technical debt & aging infrastructure	34%	35%	↓
IoT	21%	26%	↓
AI & machine learning (including generative AI)	17%	14%	↑

*Percentages reflect the number of respondents who rated the organization's level of preparedness a 4 or 5 on a 5-point scale, where 1 indicates "Not prepared at all" and 5 indicates "Extremely prepared."

Perceived threat of technology risks in next 12 months — perspectives among IT audit groups that use cybersecurity tools*

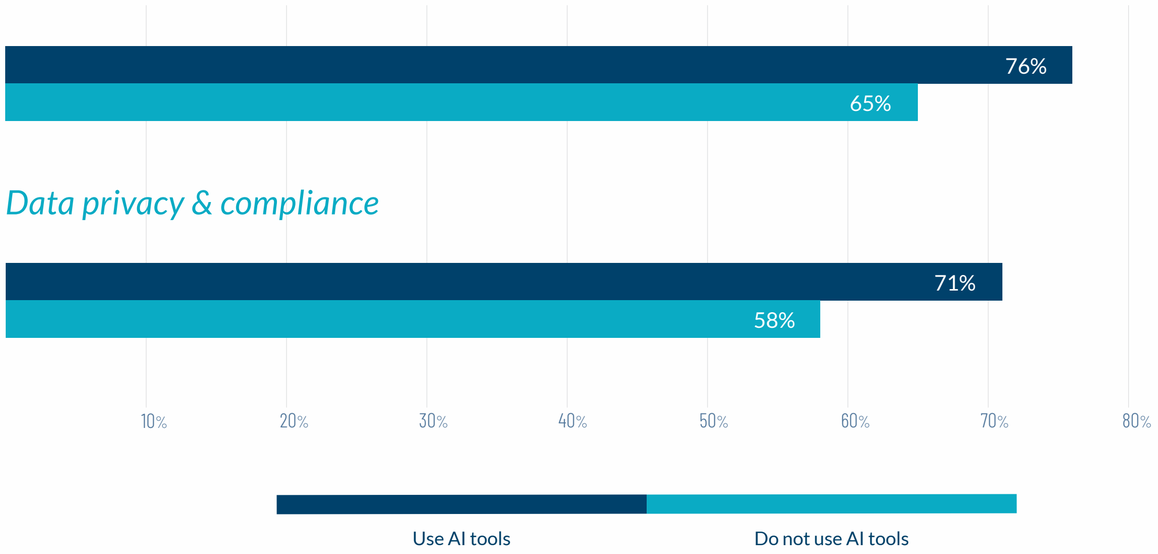
Figure 4



*Percentages reflect the number of respondents who rated the threat a 4 or 5 on a 5-point scale, where 1 indicates "No threat at all" and 5 indicates "Significant threat." See page 35 for full survey results on use of tools, technologies and delivery methods.

Perceived threat of technology risks in next 12 months — perspectives among IT audit groups that use AI tools*

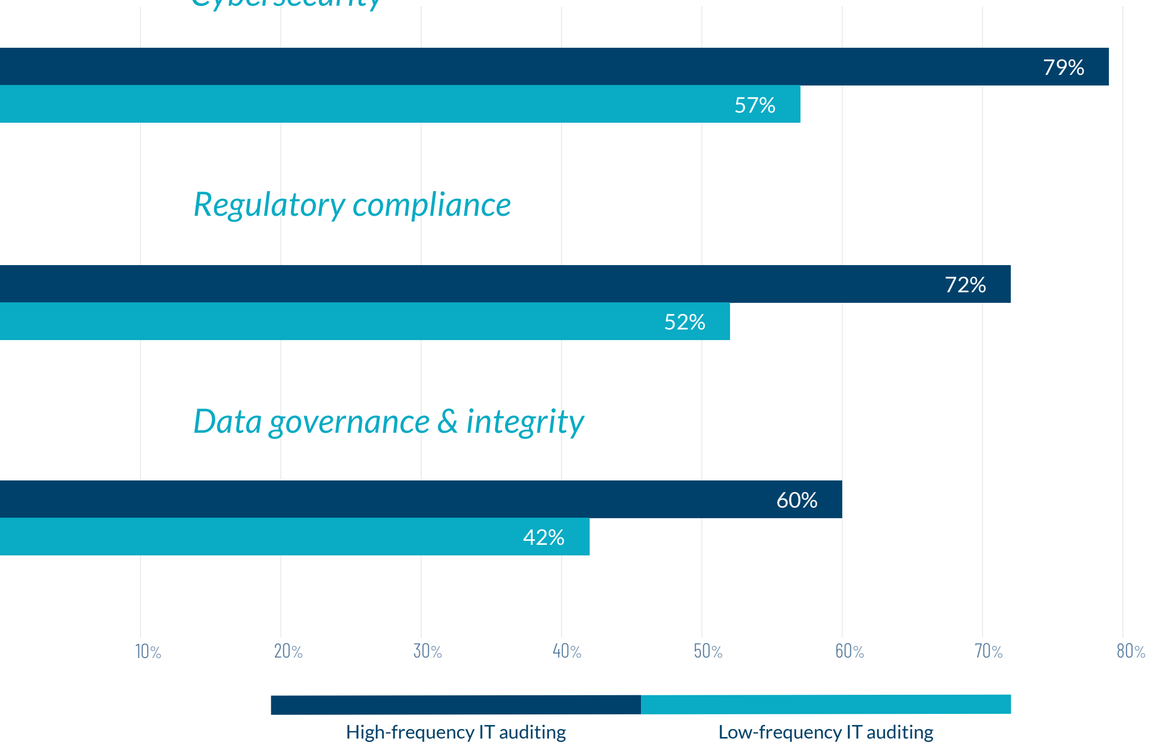
Figure 5



*Percentages reflect the number of respondents who rated the threat a 4 or 5 on a 5-point scale, where 1 indicates "No threat at all" and 5 indicates "Significant threat." See page 35 for full survey results on use of tools, technologies and delivery methods.

Perceived level of organizational preparedness to handle technology risks in next 12 months — perspectives among high-frequency IT auditing groups*

Figure 6



*Percentages reflect the number of respondents who rated the organization's level of preparedness a 4 or 5 on a 5-point scale, where 1 indicates "Not prepared at all" and 5 indicates "Extremely prepared."

Organizations that audit more frequently have a greater perception of risk

This year's findings, as well as year-over-year trends, reveal a clear takeaway: Increased frequency of technology audits performed annually drives a better understanding of key technology risks such as cybersecurity, data privacy and compliance, and data governance and integrity.

Several factors could explain this. The first — and arguably the most significant — is increased awareness and visibility. When audits are conducted more frequently, organizations are more likely to uncover risks, vulnerabilities and control weaknesses that might otherwise go unnoticed. Further, as companies become more attuned to the dynamic nature of technology and cyber risks, their perception of risk heightens. Risks can change and evolve quickly. Finally, there may be cultural factors at play. Organizations that perform more frequent audits generally have a stronger culture of risk awareness.

The survey indicates that 43% of organizations perform two or fewer technology audits annually (see Figure 2). This statistic highlights a critical gap in risk detection and mitigation. Organizations conducting fewer audits may lack the real-time insights necessary to address rapidly evolving threats, underscoring the need for more frequent and comprehensive technology audits to enhance the organization's risk posture.

"Cybersecurity continues to be a major concern for most organizations. While many internal auditors do not focus exclusively on information technology, it is becoming increasingly important that they are aware of cyber-related risks. There is an element of cybersecurity in most business processes, highlighting the need for internal auditors to identify cyber risks during the engagement risk assessment."

– **George Barham**
Director of Standards and Professional Guidance, The IIA

Perceived level of IT audit team proficiency to evaluate technology risks effectively in next 12 months (all respondents)*

Table 3

	2024	2023	YOY trends
Cybersecurity	58%	53%	↑
Data privacy & compliance	56%	52%	↑
Regulatory compliance	55%	54%	↑
Data governance & integrity	45%	49%	↓
Cloud computing	41%	34%	↑
IT talent management	39%	31%	↑
Transformations & system implementations	39%	44%	↓
Technology resiliency	38%	47%	↓
Software development	34%	35%	↓
Third parties/vendors	33%	48%	↓
Technical debt & aging infrastructure	31%	42%	↓
IoT	17%	22%	↓
AI & machine learning (including generative AI)	13%	14%	↓

*Percentages reflect the number of respondents who rated their IT audit team's proficiency level a 4 or 5 on a 5-point scale, where 1 indicates "Not at all proficient" and 5 indicates "Extremely proficient."

Comparing perceived threats with organizational preparedness and technology audit proficiency

There is a noteworthy and insightful connection between how organizations perceive various technology risks and their corresponding levels of preparedness and proficiency in managing these risks within their technology audit functions.

The most significant gaps are in the areas of third-party/vendor risks, and AI and machine learning, including generative AI. The percentages below reflect the number of respondents who rated the level of threat, organizational preparedness or technology audit function proficiency a 4 or 5 on a 5-point scale — see Figures 13, 14 and 15 in the Appendix for details, including definitions of scales for perceived threat, organizational preparedness and technology audit proficiency.

Third parties/vendors:

- **Perceived threat:** 50%
- **Organizational preparedness:** 36%
- **Technology audit proficiency:** 33%

Many organizations may lack the necessary frameworks or expertise to monitor and control the risks associated with external vendors effectively. These gaps highlight potential vulnerabilities in the supply chain, where a failure to manage third-party risks adequately could lead to significant disruptions or security breaches.

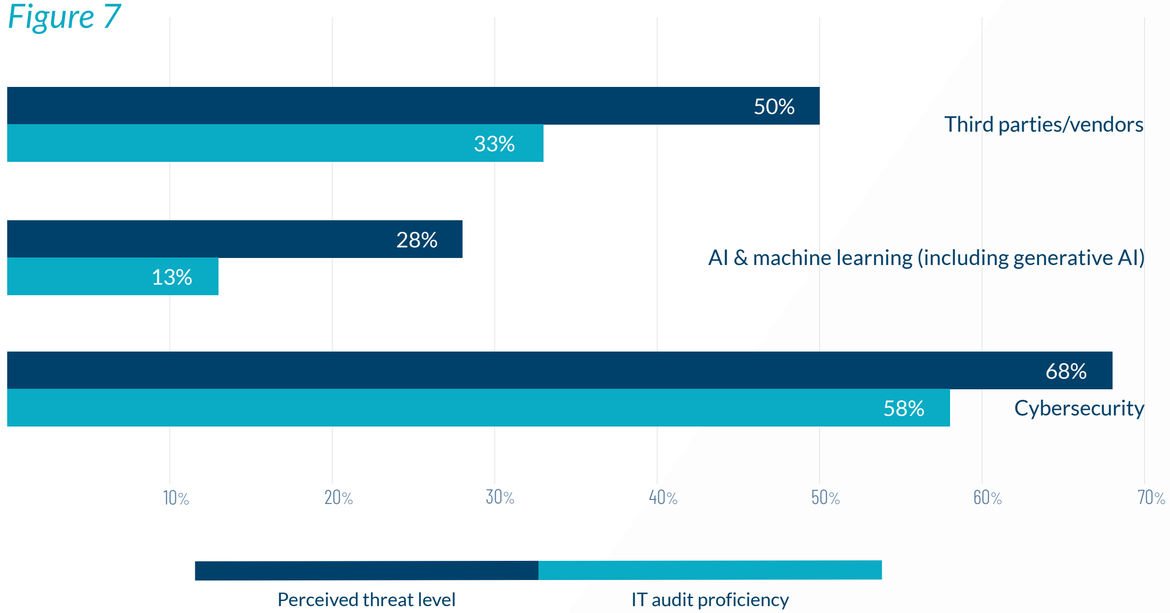
AI and machine learning (including generative AI):

- **Perceived threat:** 28%
- **Organizational preparedness:** 17%
- **Technology audit proficiency:** 13%

The gaps between the perceived threat of AI and machine learning and the levels of preparedness and proficiency are particularly concerning given the rapid adoption of AI technologies across industries. Organizations may be embracing AI without fully understanding the associated risks or developing the necessary controls to mitigate them. This leaves them vulnerable to potential ethical, security and operational challenges that could arise from AI use.

Perceived threat level vs. IT audit proficiency — top three*

Figure 7



*Percentages reflect the number of respondents who rated this threat a 4 or 5 on a 5-point scale, where 1 indicates "No threat at all" and 5 indicates "Significant threat," and the number of respondents who rated their IT audit team's proficiency level a 4 or 5 on a 5-point scale, where 1 indicates "Not at all proficient" and 5 indicates "Extremely proficient."

03

Why cybersecurity and data stand out as most significant concerns

What's top of mind: Chief concerns for IT audit leaders and teams this year include cybersecurity and a number of data-related issues — privacy, compliance, governance and integrity (see Table 1). In terms of areas of cybersecurity perceived to pose the greatest risks, data breaches and leaks of sensitive information stand out, by far, as the most significant. Following these, third-party and supply chain risks, along with cloud service provider security weaknesses, are the next most worrisome issues (see Figure 8).

Underlying regulatory factors: It's understandable to find these issues among the top technology risks, given the regulatory attention they continue to draw and the increased levels of preparedness to manage them.

In the United States, for example, the new cybersecurity disclosure rules from the Securities and Exchange Commission (SEC) have placed a spotlight on being more diligent and mindful regarding cyber risks. The rules increase reporting and disclosure requirements for companies registered with the SEC. Among the requirements, organizations must file an incident report within four business days of the company's materiality determination regarding a cyber incident. Organizations must provide insight into how the cybersecurity risk management functions are integrated into broader risk management systems and processes, such as risk reporting and monitoring processes used in conjunction with the enterprise risk management process.

Similarly, the Network and Information Security Directive 2 (NIS2) in the European Union has expanded the scope of the original directive to enhance cybersecurity across the entire European region by unifying national laws with common minimum requirements.

52% of technology audit leaders see data breaches and leaks of sensitive information as a major risk to their organization in the coming year.

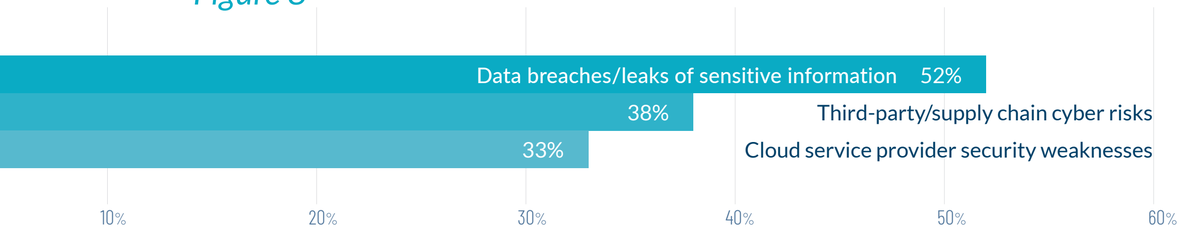
Commentary

As cyber threat actors continue to enhance the sophistication of their attack methods, IT audit teams must also continue to upskill their techniques to help management identify relevant risks. It will be increasingly difficult to keep pace without support from cyber tooling and other technology-enabled tactics. Of note, the use of tools such as vulnerability scanners and intrusion detection systems does not alleviate risk levels — in fact, they may reveal previously unknown risks and vulnerabilities. There have been situations where an organization, after employing threat detection technology, realized they were "flying blind" prior to using them. Another important point: Privately held companies may also see value in enhancing their incident identification, evaluation and remediation practices through greater use of technology tools by the IT audit function, even if they are not subject to the same public disclosure requirements.

Also, as organizations increasingly rely on data-driven decision-making, technology audit functions must evolve to provide more rigorous assessments of data governance frameworks, verifying that data integrity is maintained across both internal processes and third-party interactions.

Greatest cyber risks to organizations over next 12 months

Figure 8



As cyber threat actors continue to enhance the sophistication of their attack methods, IT audit teams must also continue to upskill their techniques to help management identify relevant risks. It will be increasingly difficult to keep pace without support from cyber tooling and other technology-enabled tactics.

04

Use of technology tools

AI on the rise: Nearly one in four IT audit functions (23%) are using AI and machine learning tools — almost double the number reported in last year's results. AI tools can provide an advantage in conducting full population testing and help to identify where sensitive data resides in the organization — sometimes in unexpected places such as in text fields within forms (see Figure 16).

Different technologies being employed: There is increased adoption of technologies such as cybersecurity tools and cloud-based audit management software. Additionally, although the usage has not increased compared with last year's results, many IT audit functions continue to employ data analytics tools (see Figure 16).

Commentary

Internal audit functions must strive to become more technology-enabled by employing tools such as AI and data analytics, among others, to deliver improved and more detailed insights into various business processes and activities.

According to findings from the Internal Audit Foundation's *Internal Audit: Vision 2035 — Creating Our Future Together* [1], new and emerging technologies are expected to have a major impact on the profession. The project's survey results (n=6,506) revealed that 96% of respondents believe internal auditors will need to increase their technology skills to stay relevant, 93% think that the use of new technology will offer better insights for their recommendations, and 92% consider new technology essential for internal audit to add more value.

As new technologies like generative AI tools are expected to impact internal audit functions significantly in the coming years, they will also affect every other function in the organization. However, internal audit functions have a unique role to play in shaping and governing the use of AI throughout an organization. Further, by integrating AI across the internal audit lifecycle (in planning, fieldwork, reporting and follow-up), internal auditors are positioned to transform the way audits are performed.

Adopting new tools and techniques presents numerous challenges. Transforming and innovating within the internal audit function requires a strong commitment. Failing to leverage technology efficiently can result in slower audits, a higher risk of misalignment on focus areas, and less insightful, relevant and valuable outputs from internal audit activities. Nearly nine out of 10 (87%) survey respondents from *Internal Audit: Vision 2035* agreed that internal audit functions that do not leverage new technology will face challenges and potential failure.

Finally, it's important to remember that technology is not just a tool, nor is it the ultimate solution. Instead, technology should be viewed as an integral component for enhancing internal audit practices.

55% of IT audit functions are employing data analytics tools to support technology audits.

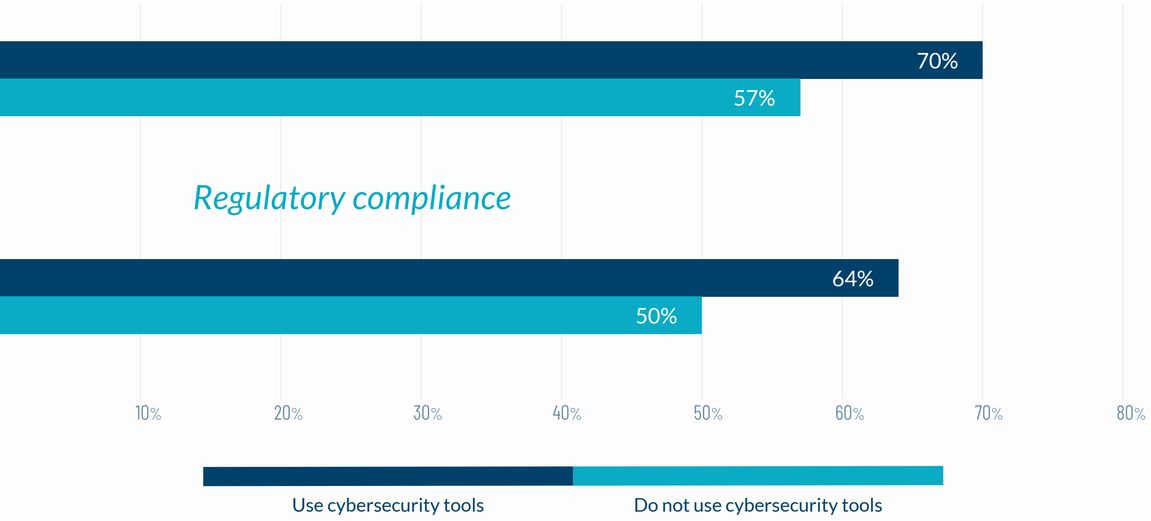
23% are using AI and machine learning tools (including generative AI), nearly double the level reported last year.

[1] "Internal Audit: Vision 2035 — Creating Our Future Together," The IIA's Internal Audit Foundation, July 15, 2024: https://ia-vision2035.org/.

Perceived level of organizational preparedness to handle technology risks in next 12 months — perspectives among IT audit groups that use cybersecurity tools*

Figure 9

Cybersecurity



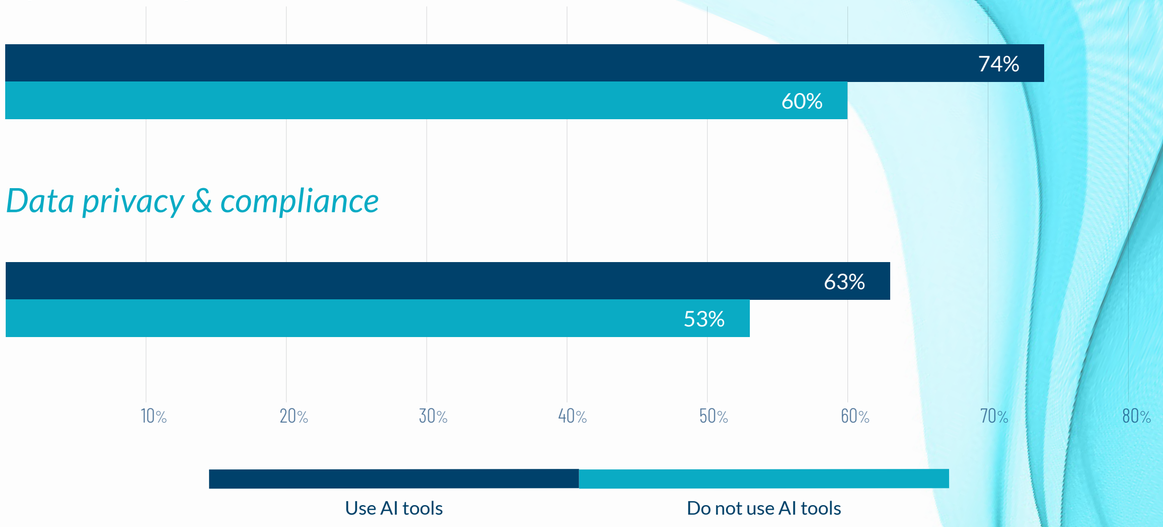
Regulatory compliance

*Percentages reflect the number of respondents who rated the organization's level of preparedness a 4 or 5 on a 5-point scale, where 1 indicates "Not prepared at all" and 5 indicates "Extremely prepared."

Perceived level of organizational preparedness to handle technology risks in next 12 months — perspectives among IT audit groups that use AI tools*

Figure 10

Cybersecurity



Data privacy & compliance

*Percentages reflect the number of respondents who rated the organization's level of preparedness a 4 or 5 on a 5-point scale, where 1 indicates "Not prepared at all" and 5 indicates "Extremely prepared."

05

A closer look at AI and IT audit

AI is the focus of the longer-term outlook for emerging risks: While IT audit leaders and professionals do not view AI as presenting a high level of risk over the next 12 months (see Table 1), their views change when looking further ahead. A majority of respondents see advanced AI systems as posing significant risks to the business over the next two to three years (see Figure 11) — far more than other emerging technologies, such as advanced IoT systems.

A majority of organizations (59%) believe advanced AI systems (including generative AI) will pose significant risks in the next two to three years.

Security and privacy top the list of AI risk concerns: A majority of respondents see security risks such as hacking, adversarial attacks and data poisoning to be the most significant AI-related risks over the next 12 months. Privacy risks such as data misuse and consent violations also rank highly. This is understandable given the rapid rise in the use of AI, including generative AI systems, throughout organizations without, in many cases, commensurate levels of governance, controls and oversight over data use and security protocols.

Internal audit is engaged in AI opportunities: In most organizations, the internal audit function is involved in researching the future use of AI (see Figure 19). This is a positive development, considering the integral role that IT and internal audit functions play in assessing that AI is implemented effectively, efficiently and in a controlled manner throughout the enterprise. To achieve success, the internal audit function will require a strong understanding of how to use AI within its own activities.

Top 3 AI-related activities in which the internal audit function is involved

52% Researching future use of AI

39% Auditing use of AI in the organization

39% Using AI for internal audit activities

Commentary

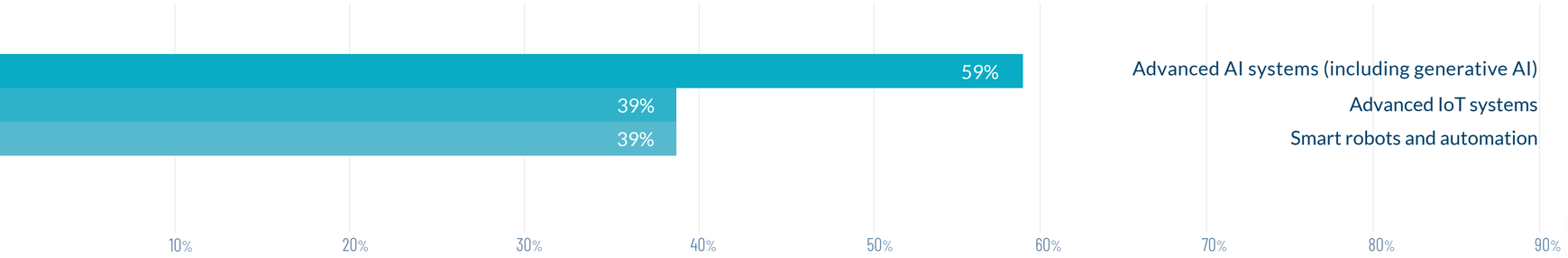
Audit leaders and professionals seem less concerned about AI risks in the next 12 months (see Table 1) compared to the two- to three-year outlook (see Figure 11). One possible reason behind the 12-month numbers could be a lack of understanding of the risks and how the organization is using or planning to use AI. This suggests a need for organizations to drive more preparedness to handle AI-related risks and to build technology audit proficiency in these areas to be ready for the future.

Although AI is not perceived to be a significant short-term risk, audit leaders should proactively assess the ethical, operational and reputational challenges it poses (especially considering the velocity of adoption in the market). CAEs should give AI immediate attention, focusing on determining whether their organizations are establishing governance and leveraging frameworks (e.g., the NIST AI Risk Management Framework) to enable readiness for more sophisticated AI implementations.

Looking at the most significant risk concerns around the use of AI, it's likely that the technology will increasingly raise security and privacy concerns, particularly around data, in the future. As AI becomes more ingrained in businesses and for personal use worldwide, new data security and privacy concerns are likely to emerge alongside these technological advancements.

Emerging technologies expected to pose most significant risks in the next 2-3 years

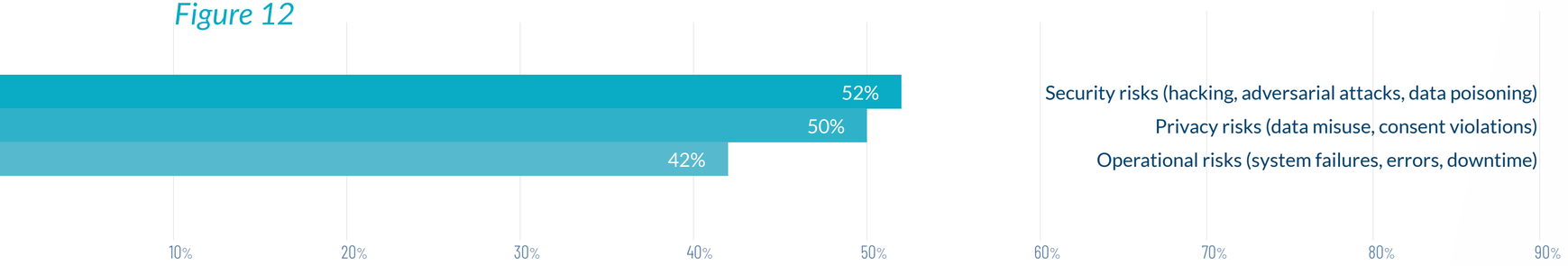
Figure 11



Respondents selected up to three answers — top three shown. See Figure 19 for a full list of responses.

Greatest risks related to AI over next 12 months

Figure 12



Respondents selected up to three answers — top three shown. See Figure 20 for a full list of responses.

06

Our call to action for technology audit leaders and teams

This year's research results point to several important actions that CAEs and technology audit leaders and teams should take to address today's and tomorrow's technology challenges and position their organizations for success.

Increase the frequency of technology audits performed annually. Audit groups that conduct six or more technology audits annually perceive some technology risks as more significant threats to the business compared to low-frequency IT auditing groups. Moreover, they have more positive views of the levels of preparedness in organizations to manage technology risks. Some organizations continue to conduct just one technology audit every year. The path forward in technology auditing begins with performing more detailed, technology-enabled and thorough IT audits across the enterprise on an annual basis. IT audit teams also should focus on upskilling or exploring other ways to evaluate technology risks more consistently.

Assess technology audit proficiency gaps. The survey results reveal significant gaps between perceived threat levels and proficiency levels for a number of technology risks, including third-party risk and AI. Technology audit functions need to prioritize elevating their proficiency in these areas. To accomplish this, organizations should focus on providing tailored training for their audit teams, including certification programs, hands-on workshops and collaborative exercises with IT departments. Internal audit leaders also should foster knowledge-sharing initiatives and encourage cross-functional teams to work together to increase technical expertise and domain knowledge, particularly in rapidly evolving areas like AI and cloud security. Notably, understanding and addressing discrepancies between perceived threats and actual capabilities is crucial for strategic planning. By identifying these gaps, organizations can prioritize their efforts and resources more effectively. Such a targeted approach not only mitigates potential risks but also enhances overall resilience and readiness in an increasingly complex technology landscape.

Embrace the use of advanced tools in technology auditing. Leveraging technology tools such as AI for risk prediction, anomaly detection and text generation, along with cybersecurity tools like vulnerability scanners, provides a clearer understanding of the threat landscape. This approach also fosters more positive perceptions of an organization's preparedness to manage current and emerging threats.

Stay laser-focused on cybersecurity. IT audit leaders and teams view cyber threats as the top technology risk for organizations, by a large margin. These threats drive concerns over breaches, leaks of sensitive information and long-term reputation damage. While cybersecurity remains a front-and-center issue for technology auditors, they must stay current not only on the latest specific cyber threats but also on the tools and technologies that can help organizations defend against and combat these threats.

Stay on the leading edge of AI. The exponential growth in the use of AI will continue. Technology audit leaders and teams must stay closely attuned to how AI is being deployed throughout the enterprise to monitor effective use and identify potential risks. They must also ensure that appropriate controls and governance are in place so that data privacy and security risks are managed appropriately and ethical use of these technologies is evaluated. Additionally, they should look for opportunities to incorporate AI into their audits, which will enhance their overall precision and effectiveness. Organizations should provide targeted training to audit and risk management teams to enhance their understanding of AI technologies and the unique risks they pose. This will help build internal proficiency and enable more effective oversight.

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:

- GTAG Assessing Cybersecurity Risk
- GTAG Cyber Incident Response and Recovery
- GTAG Cybersecurity Operations Prevention and Detection
- GTAG Auditing Mobile Computing
- GTAG Understanding and Auditing Big Data
- The IIA's Auditing Artificial Intelligence Framework

Don't forget data. While cybersecurity stands out as the most significant risk concern for technology audit leaders and teams, there are a number of data-related issues as well — among them, privacy, governance, integrity and compliance. There also are growing data-related concerns pertaining to the increasing use of AI. Technology audit teams must remain focused on these data issues and ensure they have access to the right data from the enterprise. This access is essential for performing thorough audits and delivering the deep insights and analysis expected by stakeholders.

Prioritize third-party risk management. The study highlights that third-party and vendor management represents the technology risk with the widest gap between perceived threat levels and both organizational preparedness as well as IT audit proficiency. This disparity underscores the need for audit teams to enhance their skills and capabilities in managing third-party risks, especially as organizations become more reliant on external vendors and partners. Audit leaders should develop and implement specialized training programs focused on third-party risk management. Additionally, investing in tools that offer continuous monitoring and evaluation of vendor performance and security practices is important. Audit functions should establish or refine governance frameworks that define roles, responsibilities and processes clearly for managing third-party risks. Regular audits and assessments should be conducted to ensure compliance with these frameworks.

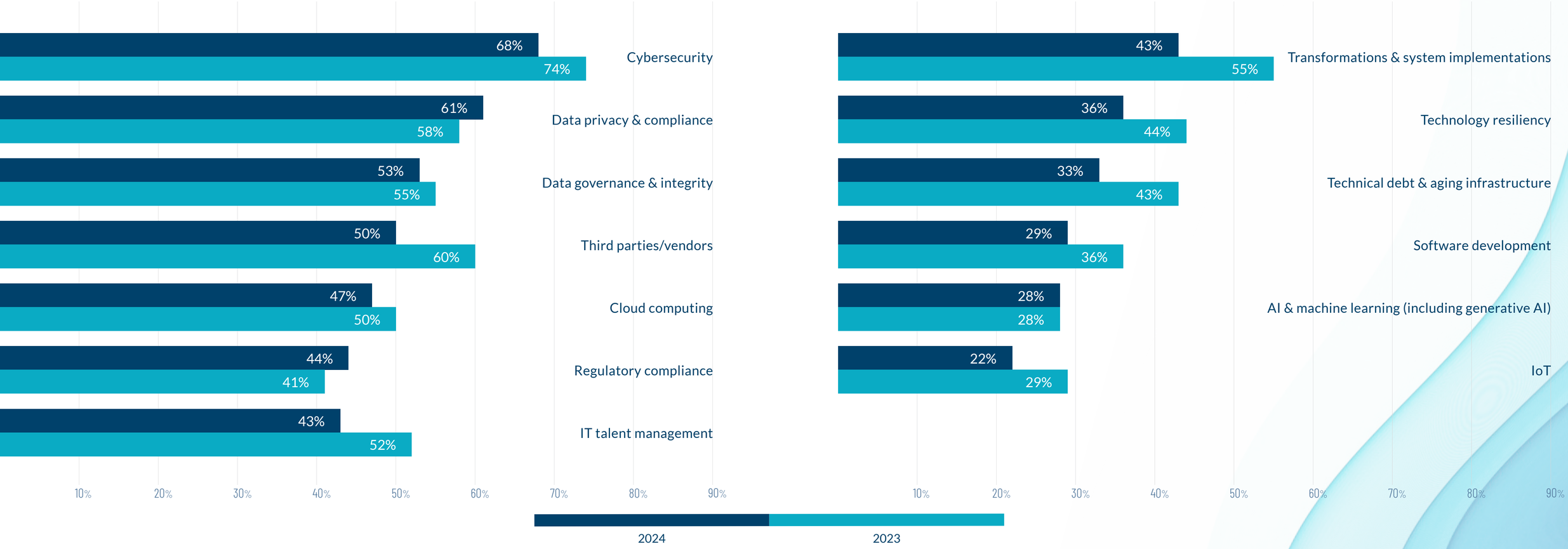
07

Appendix — full global results

Following are the full global results from our study. All data represents responses from all survey participants (n=1,246).

Perceived threat of technology risks in next 12 months

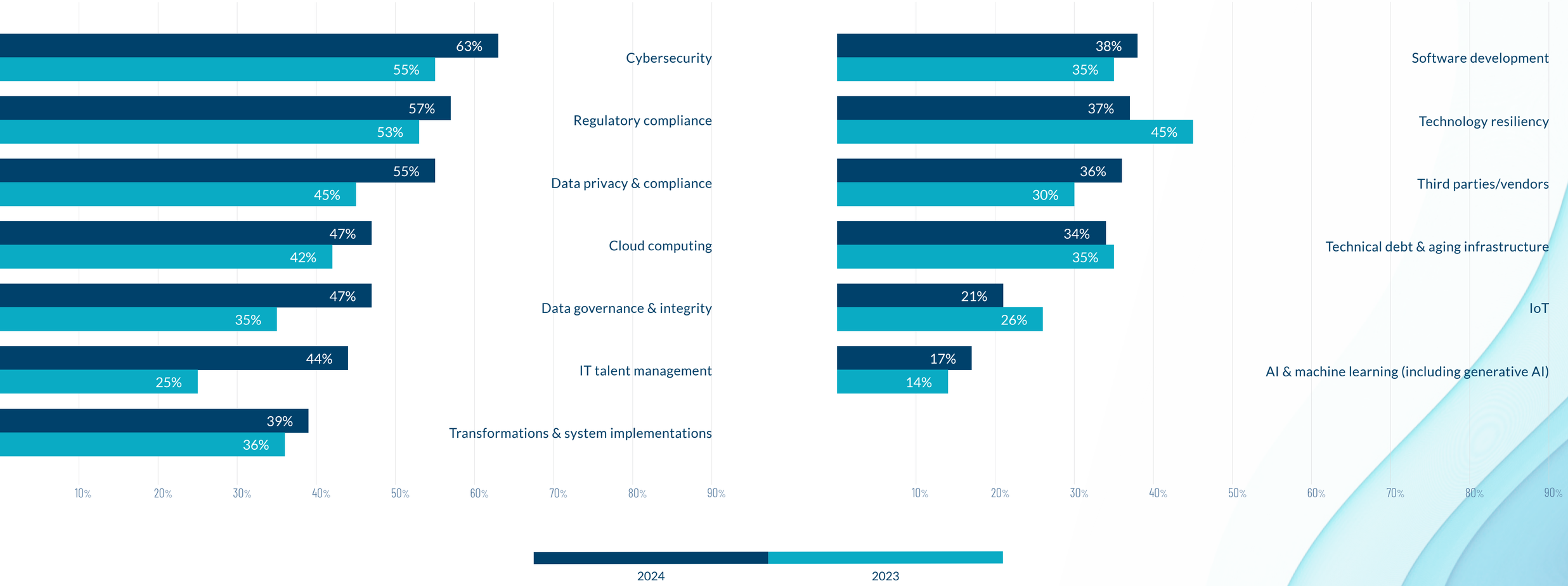
Figure 13



Question: Please rate the following technology risk in terms of the perceived threat it poses to your organization 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=1,246.

Level of organizational preparedness to handle technology risks in next 12 months

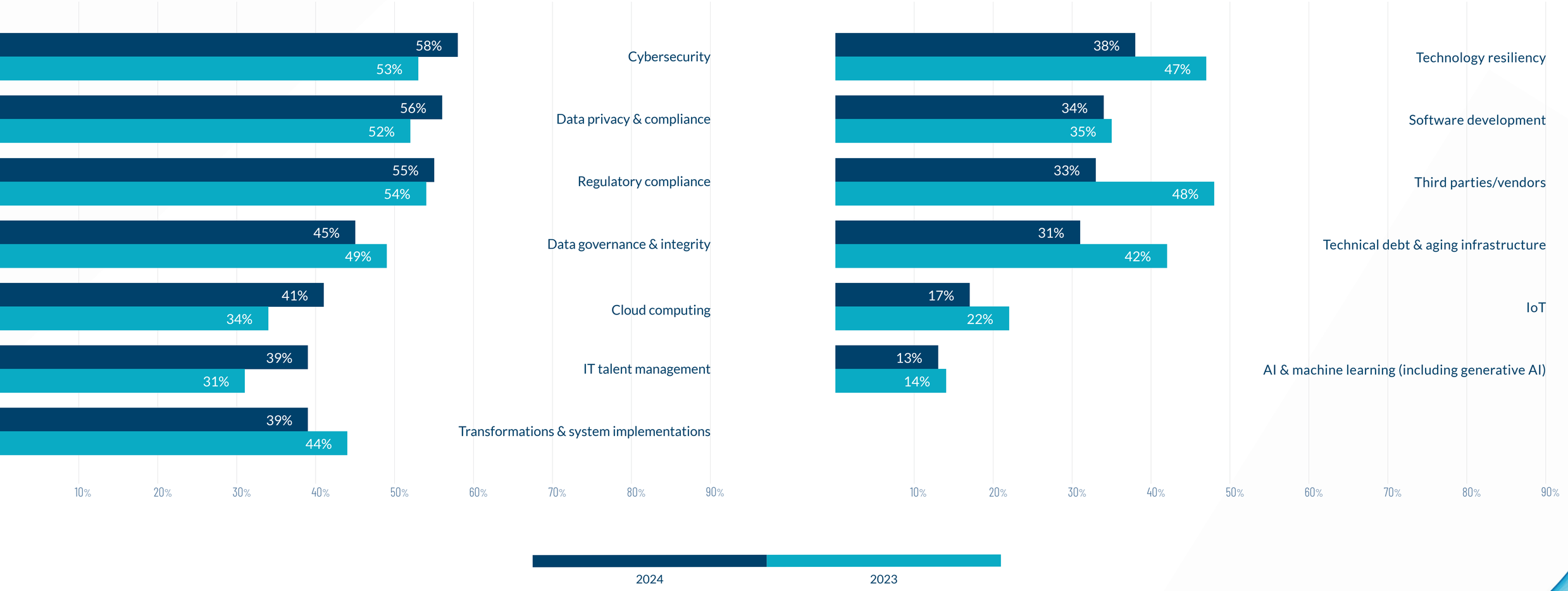
Figure 14



Question: How prepared is your organization 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=1,246.

Proficiency of IT audit team to evaluate technology risks

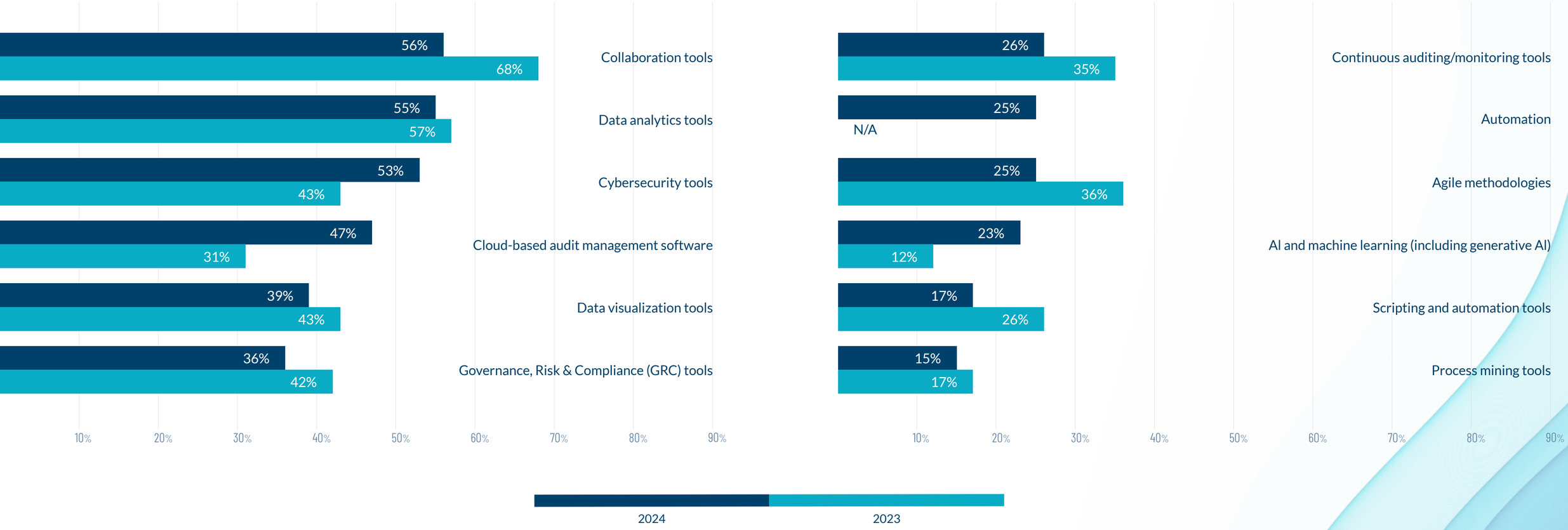
Figure 15



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=1,246.

Use of tools, technologies and delivery methods to support the IT audit function

Figure 16



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=1,246. “Other” and “None of the above” responses not shown.

Definitions of survey-assessed tools, technologies and delivery methods

AI and machine learning (including generative AI) – Using advanced algorithms and large language models like ChatGPT for risk prediction, anomaly detection, knowledge discovery, text generation and other related activities.

Agile methodologies – Applying principles of Agile (flexibility, customer-centricity, iterative progress) to the IT audit function.

Automation – Using software robots or "bots" to automate routine, rule-based tasks.

Cloud-based audit management software – Shifting audit management systems to the cloud for improved scalability, accessibility and integration.

Collaboration tools – Tools like MS Teams or Slack that enhance communication and collaboration within the IT audit team and with other teams.

Continuous auditing/monitoring tools – Implementing systems for ongoing, real-time assessment of organizational risks and controls.

Cybersecurity tools – Using tools like vulnerability scanners, intrusion detection systems and threat detection/intelligence platforms to audit the organization's cybersecurity posture.

Data analytics tools – Deploying software that can analyze large volumes of data for risk assessment, trend identification and audit planning/execution.

Data visualization tools – Using software to represent audit findings and risk assessments in a graphical, easy-to-understand format.

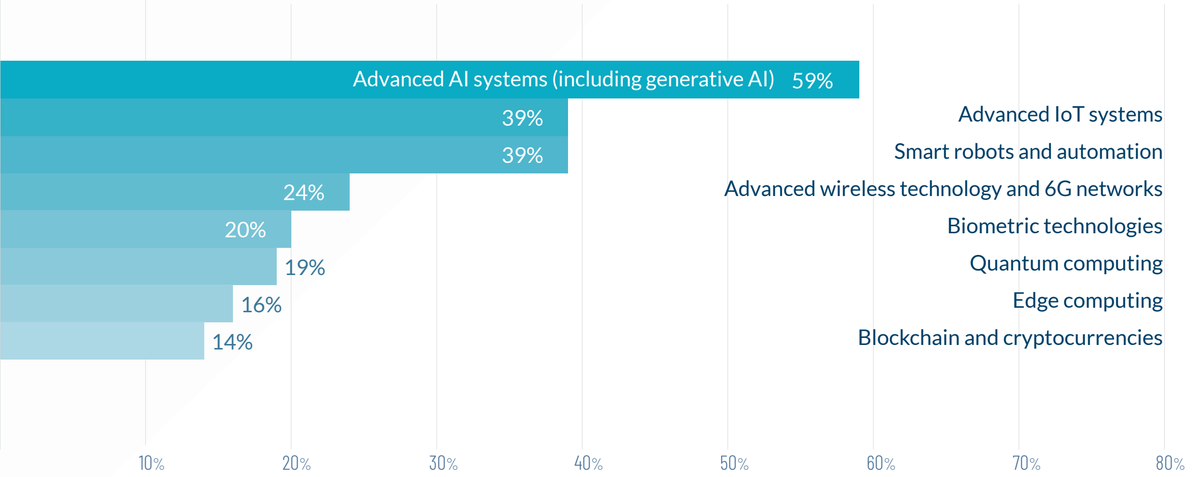
Governance, Risk and Compliance (GRC) tools – Leveraging GRC software to streamline and automate IT audit processes.

Process mining tools – Automated analysis of business and IT processes based on event logs for discovering, monitoring and improving real processes.

Scripting and automation tools – Using programming and scripting languages (e.g., Python, PowerShell, Bash) to automate routine IT audit tasks.

Emerging technologies expected to pose most significant risks

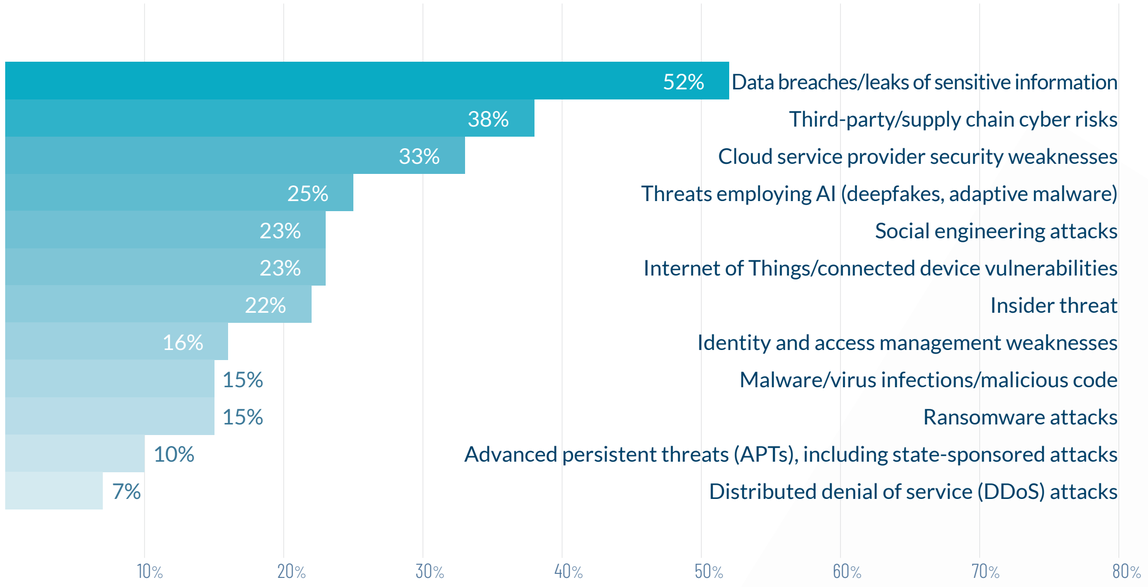
Figure 17



Question: Which of the following emerging technologies, if any, do you anticipate will pose the most significant risks to your organization in the next 2-3 years? (Up to three responses permitted.) n=1,246 — "Other" and "None of the above" responses not shown.

Most significant cybersecurity risks

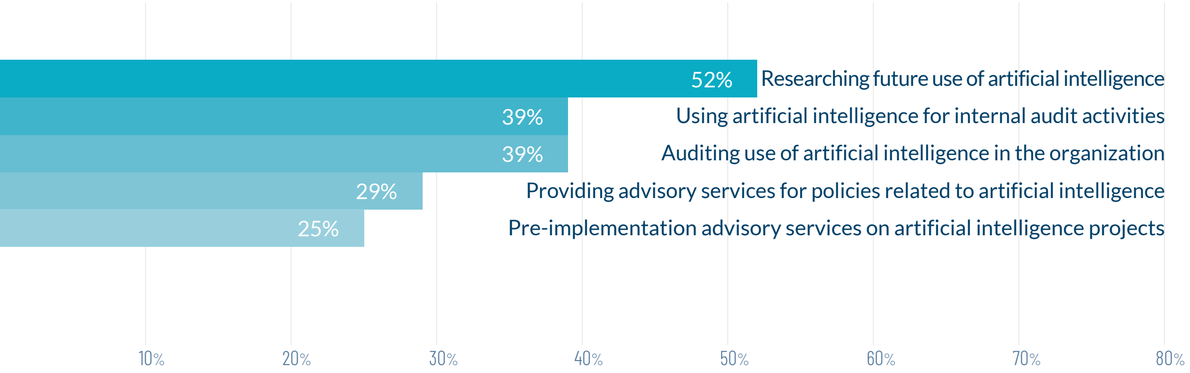
Figure 18



Question: Within the realm of cybersecurity, which of the following areas, if any, pose the greatest risks to your organization over the next 12 months? (Up to three responses permitted.) n=1,246 — "Other" and "None of the above" responses not shown.

Internal audit involvement in AI activities

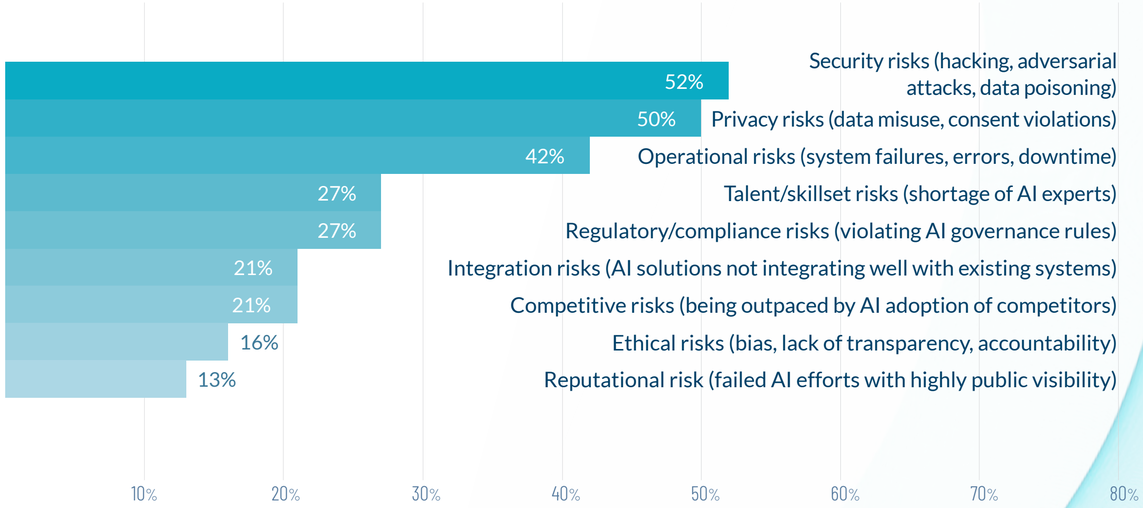
Figure 19



Question: Is your internal audit function involved in any of the following activities related to artificial intelligence? (Multiple responses permitted.) n=1,246 — "Other" and "None of the above" responses not included.

Greatest risks related to AI

Figure 20



Question: Which of the following areas related to AI (including ML and Generative AI), if any, pose the greatest risks to your organization over the next 12 months? (Up to three responses permitted.) n=1,246 — "Other" and "None of the above" responses not shown.

08

Demographics

The following tables reflect the demographics of the survey participants (n=1,246).

Position

Chief Audit Executive (or equivalent)	36%
IT Audit Director	10%
Audit Director	9%
Audit Manager	8%
IT Audit Manager	6%
IT Manager	6%
IT Executive	6%
IT Risk/Control Manager	5%
IT Risk/Control Executive	5%
IT Risk/Control Director	5%
IT Audit Staff	1%
Audit Staff	1%
Other	2%

Industry

Government	12%
Healthcare Provider	9%
Financial Services — Banking	8%
Retail	8%
Technology (Software, High-Tech, Electronics)	7%
Power and Utilities	6%
Manufacturing (other than Technology)	5%
Consumer Packaged Goods	5%
Insurance (other than Healthcare Payer)	4%
Oil and Gas	4%
Telecommunications and Data Infrastructure	4%
Financial Services — Asset Management	3%
Healthcare Payer	3%
Mining	3%
Media	3%
Transportation and Logistics	3%
Automotive	3%
Pharmaceuticals and Life Sciences	2%
Chemicals	2%
Financial Services — Broker-Dealer	1%
Financial Services — Other	1%
Wholesale and Distribution	1%
Airlines	1%
Higher Education	1%
Private Equity	1%

Organization type

Publicly traded	54%
Privately held	32%
Government	13%
Not-for-profit	1%
Other	0%

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

$20 billion or more	20%
$10 billion - $19.99 billion	14%
$5 billion - $9.99 billion	14%
$1 billion - $4.99 billion	28%
$500 million - $999.99 million	9%
$100 million - $499.99 million	10%
Less than $100 million	4%
Unsure	1%

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

$250 billion or more	40%
$50 billion - $249.99 billion	24%
$25 billion - $49.99 billion	10%
$10 billion - $24.99 billion	5%
$5 billion - $9.99 billion	5%
$1 billion - $4.99 billion	8%
Less than $1 billion	4%
Unsure	4%

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

$50 billion or more	9%
$10 billion - $49.99 billion	30%
$5 billion - $9.99 billion	13%
$1 billion - $4.99 billion	19%
$500 million - $999.99 million	14%
$100 million - $499.99 million	8%
Less than $100 million	6%
Unsure	1%

Total number of full-time technology auditors

0	5%
1	11%
2	13%
3	9%
4	7%
5	8%
6-10	19%
11+	28%

Organization headquarters

United States	35%
Canada	24%
Italy	5%
United Kingdom (UK)	4%
Australia	3%
China	3%
France	3%
Germany	3%
India	3%
Japan	3%
The Netherlands	3%
Switzerland	3%
Hong Kong	2%
New Zealand	2%
Singapore	2%
Israel	1%
Qatar	1%

About Protiviti

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

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

About The IIA

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 245,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

protiviti®

Global Business Consulting

The Institute of
Internal Auditors