IT AUDIT PERSPECTIVES ON TODAY'S TOP TECHNOLOGY RISKS

Results of ISACA/Protiviti global survey reveal cybersecurity, privacy, data and regulatory compliance are top-of-mind concerns

ISACA®

protiviti®
Global Business Consulting

Table of Contents

Executive summary

Where to begin?

The IT audit director for a large multinational conglomerate ponders this question while prioritising the organisation's lengthy list of technology risk assessments to be conducted. Many of the organisation's employees continue to work remotely, introducing a range of technical and security challenges. Cybersecurity risk always looms large and is especially critical this year given the threat of war-related cyber attacks. In addition, some of the organisation's products have been recategorised as National Critical Functions by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and, therefore, are subject to additional cybersecurity requirements. Data governance and integrity risks demand ongoing attention, as do regulatory compliance matters. Persistent staffing and attrition challenges are among other growing technology risk issues and ones that the IT audit director can relate to personally, despite time-consuming efforts to upskill the IT audit team.

This hypothetical scenario remains just as realistic if the organisation is in the telecommunications, logistics, technology, healthcare or financial services industry. An uncertain global economy, volatile geopolitical developments, a persistent pandemic, a changing regulatory landscape, and an evolving catalogue of technology risk concerns have created mounting challenges for IT audit leaders and their functions.

The results of the latest **IT Audit Technology Risks Survey** from ISACA and Protiviti, in which more than 7,500 IT audit leaders and professionals from around the world participated, show a dynamic threat landscape that has notably increased in severity since the last survey.

Key takeaways

The greatest IT audit concerns lie with cybersecurity-related breaches and related risk issues (ransomware, loss of data, etc.) — Across nearly every industry and organisation type, cybersecurity is the top-ranked technology risk. Related cyber issues such as data privacy, managing security incidents, disaster recovery, access risk and third-party risk also rate as top concerns given that they can lead to reputation damage, loss of revenue/customers and regulatory fines/scrutiny.

Data governance and data integrity are being scrutinised — These risk issues are proving difficult given the frequency and magnitude of internal changes and transformations as well as external disruptions and volatility.

Regulatory compliance burdens and risk are increasing rapidly — IT audit teams, as well as other departments (e.g., legal, compliance, IT), are scrambling to keep pace with new data privacy and data security rules as well as changing legal and regulatory compliance requirements that have growing implications for organisational data management and technology-related activities.

Top 10 technology risk factors

Cyber breach
Manage security incidents
Privacy
Monitor regulatory compliance
Access risk
Data integrity
Disaster recovery
Data governance
Third-party risk
Monitor/audit IT, legal and regulatory compliance

Given the increasingly complex and rapidly changing technology risk landscape we're in, it's imperative for IT audit leaders to understand they are responsible for maintaining a holistic view of IT risks impacting the entire organisation. This requires tech-enablement from an audit standpoint and regular calibration of risk assessments to suit the current environment, rather than rinsing and repeating the work from previous years.

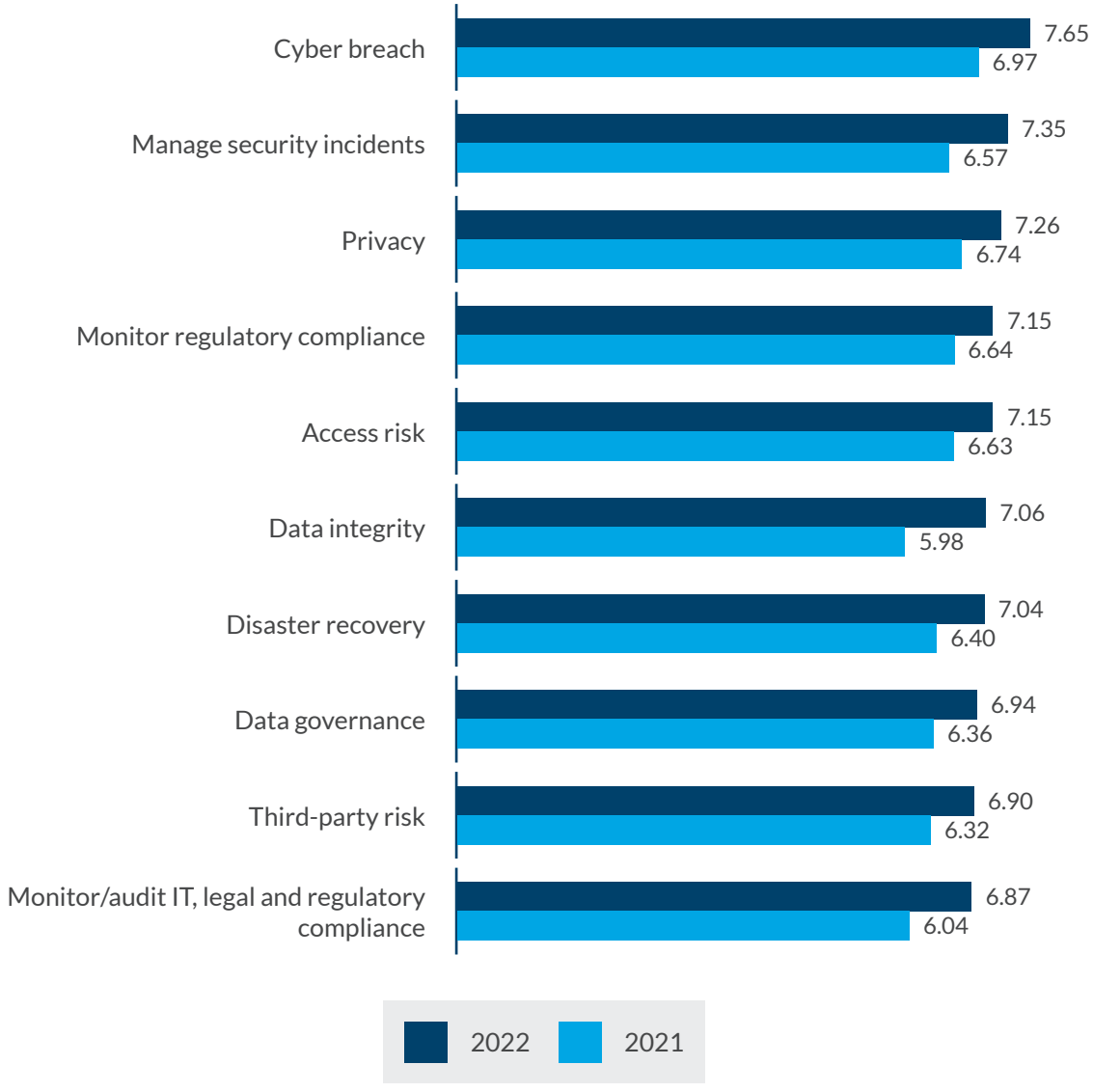
— Angelo Poulikakos, Managing Director, Global Leader, Technology Audit, Protiviti

Assessing the top technology risks

IT audit leaders and their teams have a clear understanding of the most significant technology risk issues confronting their organisations, even as the nature of these concerns, particularly those related to cybersecurity, data governance, data integrity and regulatory compliance, remain fluid and unpredictable.

One clearly apparent trend in these findings: The risk scores in this year's survey have increased significantly compared to the prior year's results, indicating perceptions that the current technology risk landscape is much riskier.

Top 10 technology risk factors



Question: *Based on your technology risk assessment, for each of the following technology risks, please rate its level of significance to your organisation using a 10-point scale, where "1" indicates low significance and "10" indicates a high significance.*

Cybersecurity — the unmistakable top technology risk

A broad range of cybersecurity-related issues — including cyber breaches, managing security incidents, privacy, disaster recovery and third-party risk — represents the top technology risk concern across nearly every industry and organisation type and in almost every country. Consider that in the handful of instances where IT audit leaders and professionals do not identify cybersecurity as the top technology risk, they rank it second. This is not surprising in light of organisations' continually expanding reliance on data and third-party partners (who use and must secure organisational data), the ongoing surge of ransomware attacks across the globe, escalating war-related cyber attacks, cloud migrations, digital transformation, new data privacy risk issues and rules, shifting data security guidance and compliance requirements — the list goes on indefinitely.

This also comes at a time when, for example, the president of the United States has warned corporate leaders at the Business Roundtable that "the magnitude of Russia's cyber capacity is fairly consequential, and it's coming" in retaliation to economic sanctions levied in response to Russia's invasion of Ukraine.[1] In fact, enhanced cybersecurity regulations and requirements continue to be enacted around the world. As another example, Australia's Security Legislation (Critical Infrastructure) Act 2021 includes numerous enhanced cybersecurity obligations.

War-related cyber attacks are far from the only threats to organisational cybersecurity capabilities that IT audit teams place a high priority on assessing and addressing this year. IT audit leaders and professionals also identify several related and significant technology issues, including data privacy, access risk, third-party risk management and disaster recovery.

Over the past year, a substantial percentage of disaster recovery efforts across many industries have been triggered by ransomware attacks. This cybersecurity risk is estimated to have cost U.S. companies $20 billion in 2021 while understandably stimulating increased vigilance among senior management teams and boards.[2] Spurred on by the EU's General Data Protection Regulation (GDPR) and similar regulatory mandates around the world, boards of directors also have sharpened their focus on data privacy. Privacy-related technology risk represents a unique challenge driven by the volume and type of data an organisation captures, retains and shares with third parties. A quickly evolving regulatory environment along with ongoing changes to business processes and IT environments further complicate this technology risk.

While IT audit teams may not be on the front lines managing these cybersecurity risk concerns, they must assess the efficacy of these efforts while ensuring that proper controls and protections are in place. Given the numerous and varied factors exacerbating cybersecurity risk, IT auditors' assessments must cast a wide net, extending from the frequency and relevancy of organisational cybersecurity training programmes to critical looks at the frameworks the organisation uses to conduct its security assessments. Leading IT audit teams certainly conduct their own holistic cybersecurity assessments to understand the framework(s) being used and whether cybersecurity risk is being managed effectively.

In a similar vein, it is important that IT audit leaders recognise the extent to which shifts inside the organisation create ripple effects of changes to technology risk. To illustrate: The widespread move to remote and hybrid working models over the past two years subjected many organisations to new

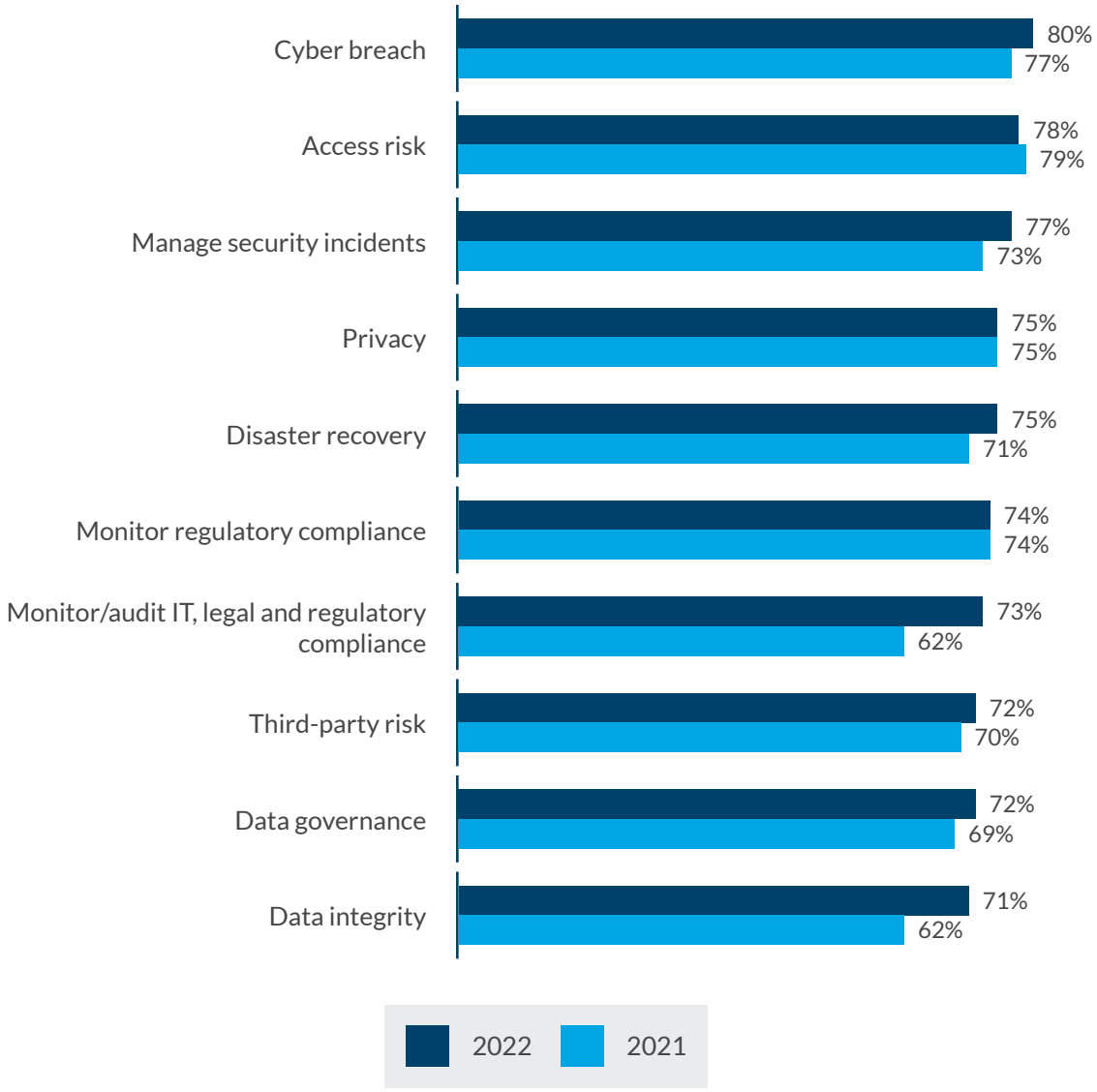
[1] "Remarks by President Biden Before Business Roundtable's CEO Quarterly Meeting," 21 March 2022: www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/21/remarks-by-president-biden-before-business-roundtables-ceo-quarterly-meeting/.

[2] "Ransomware: Analysing Risk and Protecting Critical Assets," *Board Perspectives*, Protiviti, September 2021: www.protiviti.com/US-en/insights/newsletter-bp143-ransomware.

cybersecurity risk issues. Remote work also catalysed cloud migrations in organisations of all sizes and industries. In many cases, the acceleration of cloud migrations occurred with a less-than-methodical approach to updating controls and processes to ensure cloud security.

Finally, one remarkable result from the survey is that one in five organisations do not expect their 2022 audit plans to address the risk of cybersecurity breaches. While there may be a number of possible reasons for this, such as cybersecurity risk being managed by the IT or information security function, it's important for the IT audit function to ensure cybersecurity is addressed with the appropriate risk-and-control mindset.

Expected to be addressed in the 2022 audit plan



Data governance and integrity — the core of many technology risk concerns

Organisations are collecting and using more data from more sources, many of them new ones, while sharing their data with more third-party partners. The growing number of benefits that organisations gain from data means that a larger proportion of organisational value hinges on how well this data is managed and secured. This explains why IT audit leaders and professionals identify a number of data-related technology risk factors, such as data governance and data integrity, among their top concerns this year and score them at a significantly higher level compared with the prior year results.

The nature of data governance and data integrity risk remains unsteady due to a combination of internal business changes (e.g., digital transformation, cloud migration, hybrid work and the ongoing talent crunch) and external disruptions (e.g., the global ripple effects of Russia's war on Ukraine, supply chain upheaval and cyber attackers) that hinder an organisation's ability to govern and protect its data.

This explains why, according to the survey results, more than seven in 10 organisations are addressing data governance and data integrity in their audit plan. This finding raises an important question for the significant number of organisations that are not doing so: Why not? If organisations are not addressing data governance and integrity in their audit plan, auditors should consider and perform alternatives to audits to lend assurance in these critical areas.

As IT audit leaders and teams look closely at data governance and data integrity risk in their organisations, they will want to keep in mind several interrelated factors, including the growing reliance on third-party partners, the continued enactment of data privacy regulations such as GDPR happening around the world, and the fact that increasingly frequent staffing and technology changes have direct impacts on data governance and data integrity processes and risk.

Talent and retention challenges are especially prevalent amid the current "Great Resignation" or "Great Reshuffle." As data privacy regulatory compliance burdens rapidly expand, many organisations are experiencing difficulty hiring and retaining data privacy professionals: 55% of global respondents to ISACA's 2022 State of Privacy survey indicate that their organisations are experiencing technical privacy staffing shortages. Legal and compliance privacy skills are also in short supply: 46% of respondents to the same survey are experiencing staffing shortages in this area, underscoring the challenges many IT audit groups face in addressing and managing data-related technology risk effectively.[3]

For practitioners auditing data governance and data integrity as well as those who are not, the opportunity to reinforce the criticality of these areas is real. In addition to audits, self-assessments and awareness training can emphasise the role that the entire organisation plays in addressing technology risk associated with data.

— Paul Phillips, Director of Event Content Development, ISACA

[3] Isaca.org, "Privacy in Practice 2022," 2022: www.isaca.org/resources/white-papers/privacy-in-practice-2022.

Regulatory compliance — a moving target given evolving requirements globally

Data privacy regulations are among many regulatory compliance-related risk factors IT auditors must assess as they strive to monitor an expanding global set of IT, legal and regulatory requirements and then determine the extent to which organisational processes and controls satisfy those requirements.

Compliance requirements, more often than not, impact the entire enterprise. They relate to data privacy and data security, industry standards, national and regional requirements, and even the sudden, sweeping and unprecedented economic sanctions levied against Russia in response to its invasion of Ukraine. "Banks, which have long been on the financial-crimefighting front line, will find complying tricky but manageable," according to *The Economist*. "The challenge is more daunting for non-financial companies, a far greater number of which do business that is covered by the sanctions than was the case with Iran or other past [sanctions] programmes."[4]

The extension of new legal and regulatory requirements to new industries and types of organisations exists across a number of regulatory compliance areas. IT audit groups must recognise these developments and their implications. In response to intensifying cyber attacks, more governments have expanded the types of organisations that qualify as "critical infrastructure" and are therefore subject to more stringent cybersecurity requirements. This includes the United States, which now identifies 55 "National Critical Functions" that can make an organisation subject to CISA guidance.[5] And as noted earlier, Australia's Security Legislation (Critical Infrastructure) Act 2021 includes numerous enhanced cybersecurity obligations.

In many organisations, IT auditors will be assessing risk related to regulatory requirements that their colleagues are striving to comply with for the first time, and often without the mature compliance capabilities that reside in heavily regulated industries such as financial services. IT audit teams need access to reporting data, systems, processes, controls and staffing (levels and skills) to assess rapidly changing compliance risk effectively.

As new regulatory requirements surface, IT auditors' understanding of the business positions them to assess gaps between new expectations and current practices. This is forward thinking in action that can minimise compliance fatigue by relying on existing controls where possible.

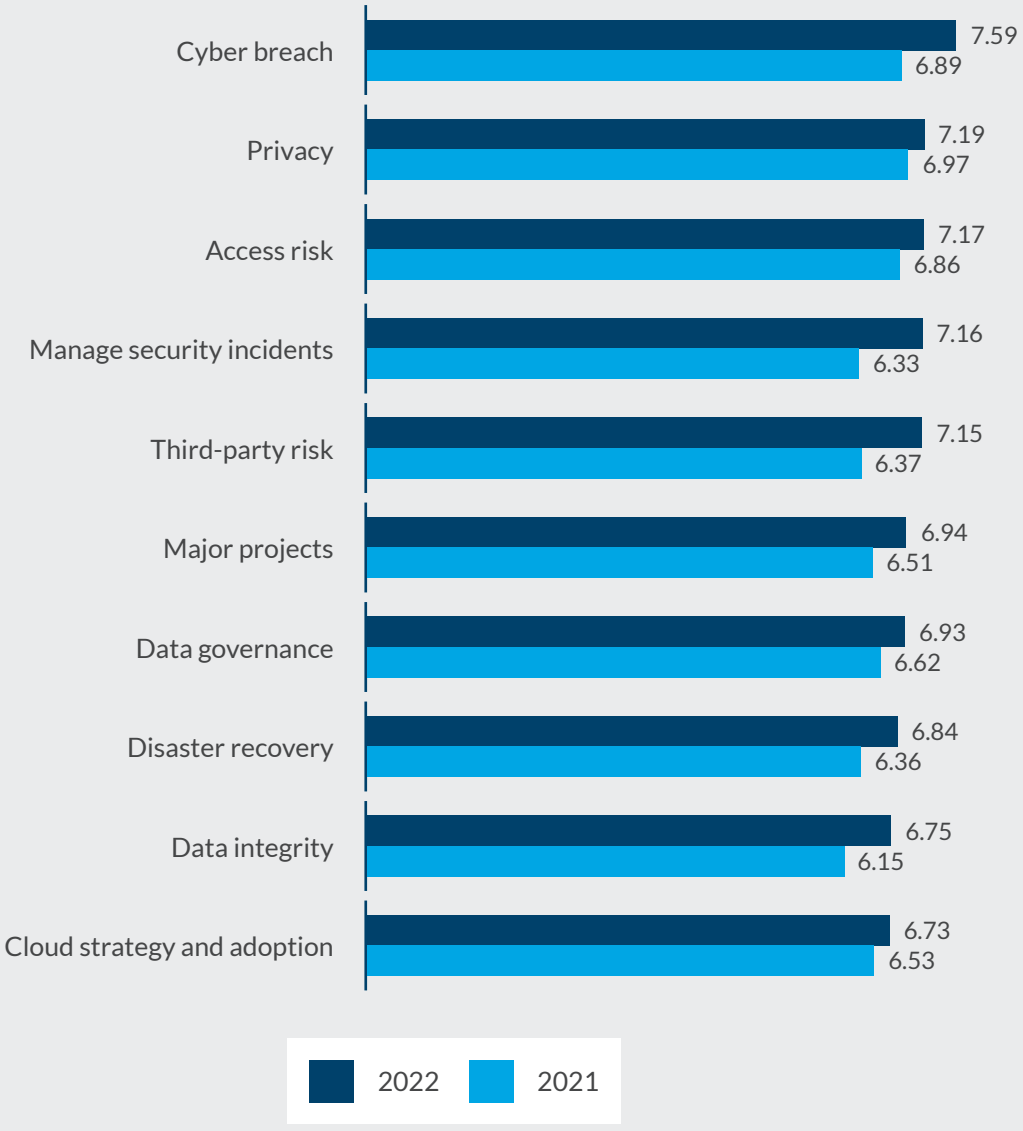
— Robin Lyons, IT Audit Professional Practices Principal, ISACA

[4] "Banks and firms face a mammoth sanctions-compliance challenge," *The Economist*, 19 March 2022: www.economist.com/business/2022/03/19/banks-and-firms-face-a-mammoth-sanctions-compliance-challenge.

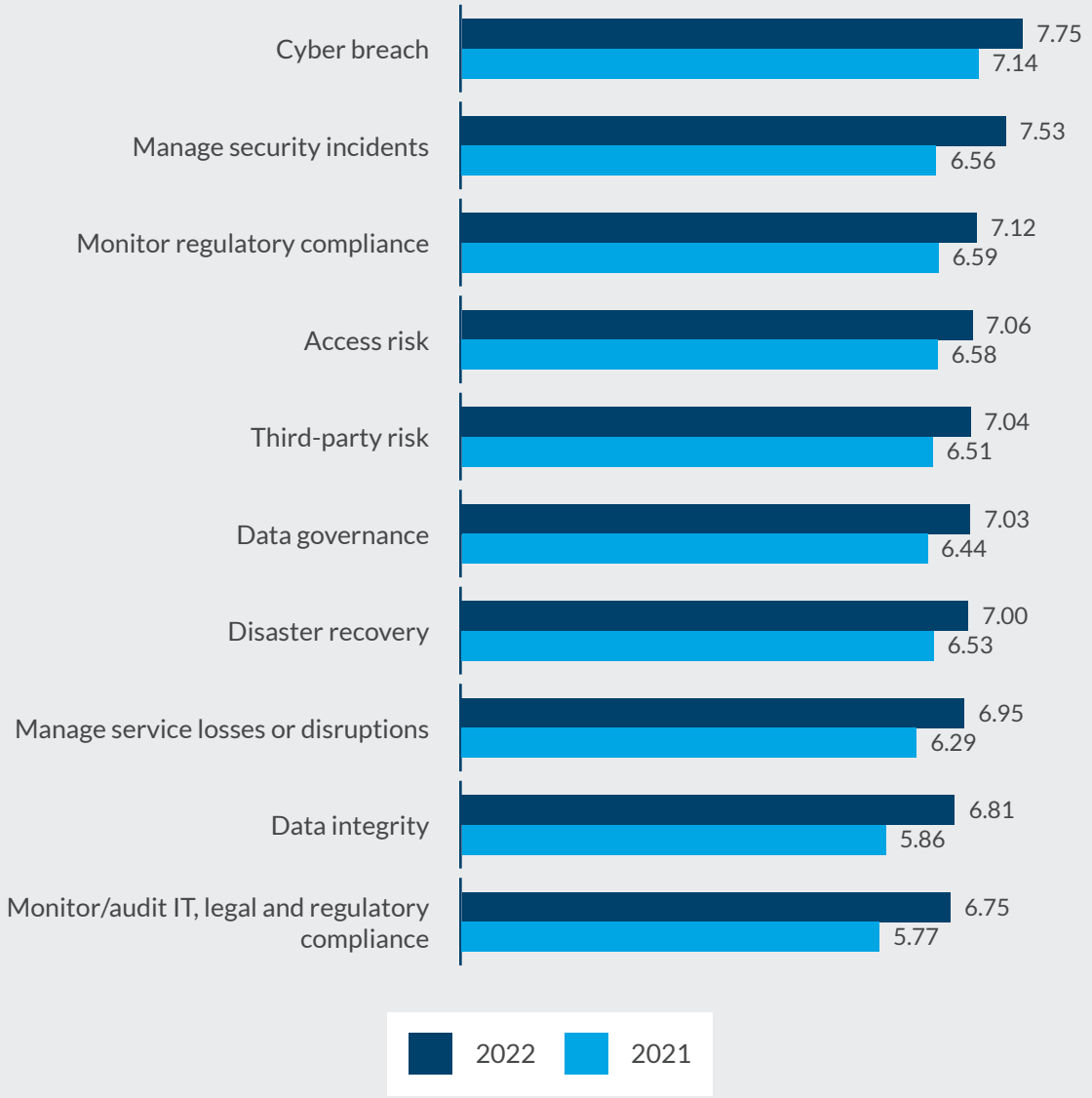
[5] "Status Update on the National Critical Functions," memorandum from Bob Kolasky, Assistant Director, Cybersecurity and Infrastructure Security Agency, 15 December 2021: www.cisa.gov/sites/default/files/publications/2021_ncf-status_update_508.pdf.

Top 10 technology risk factors by industry group

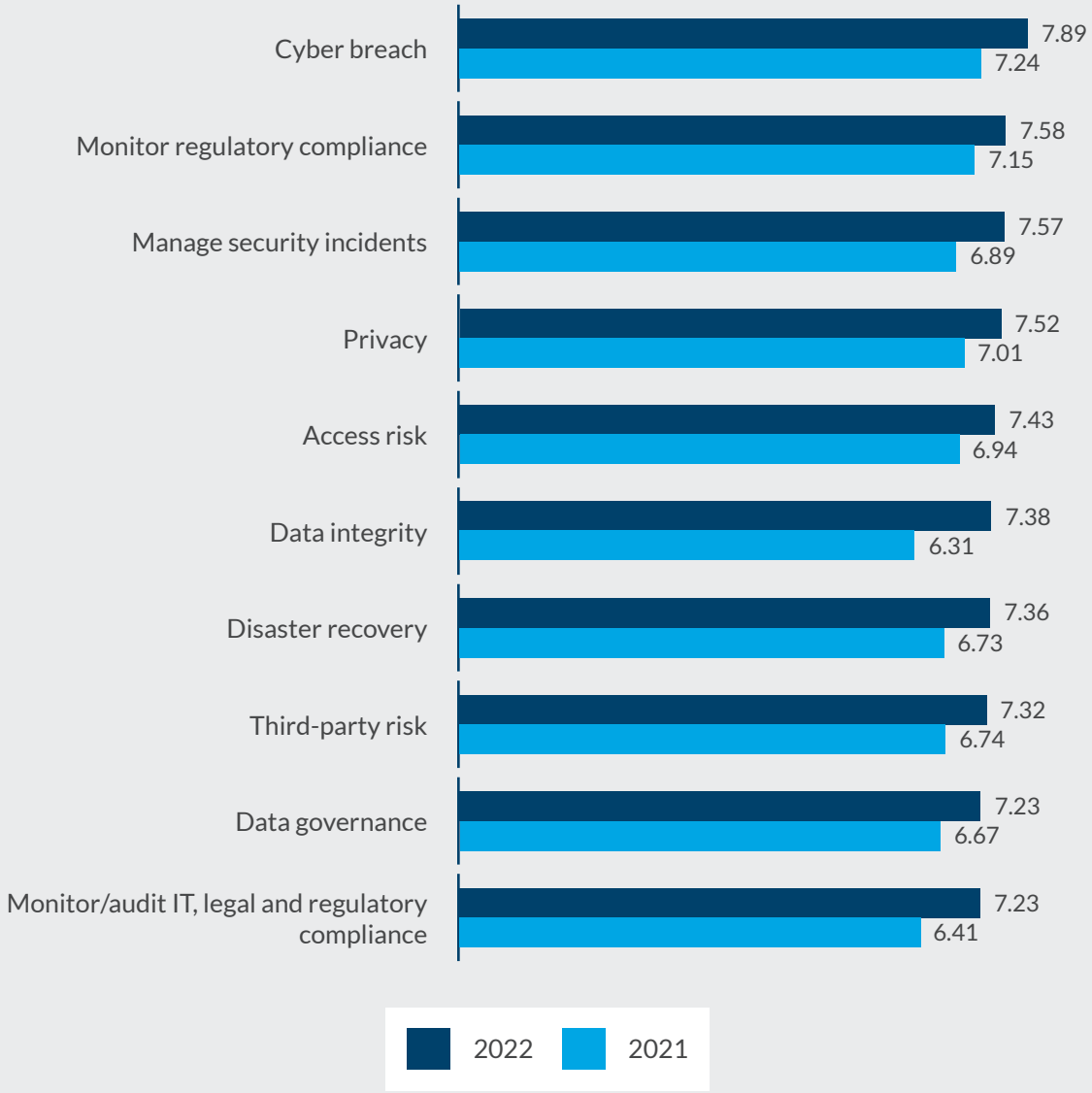
Consumer packaged goods/retail



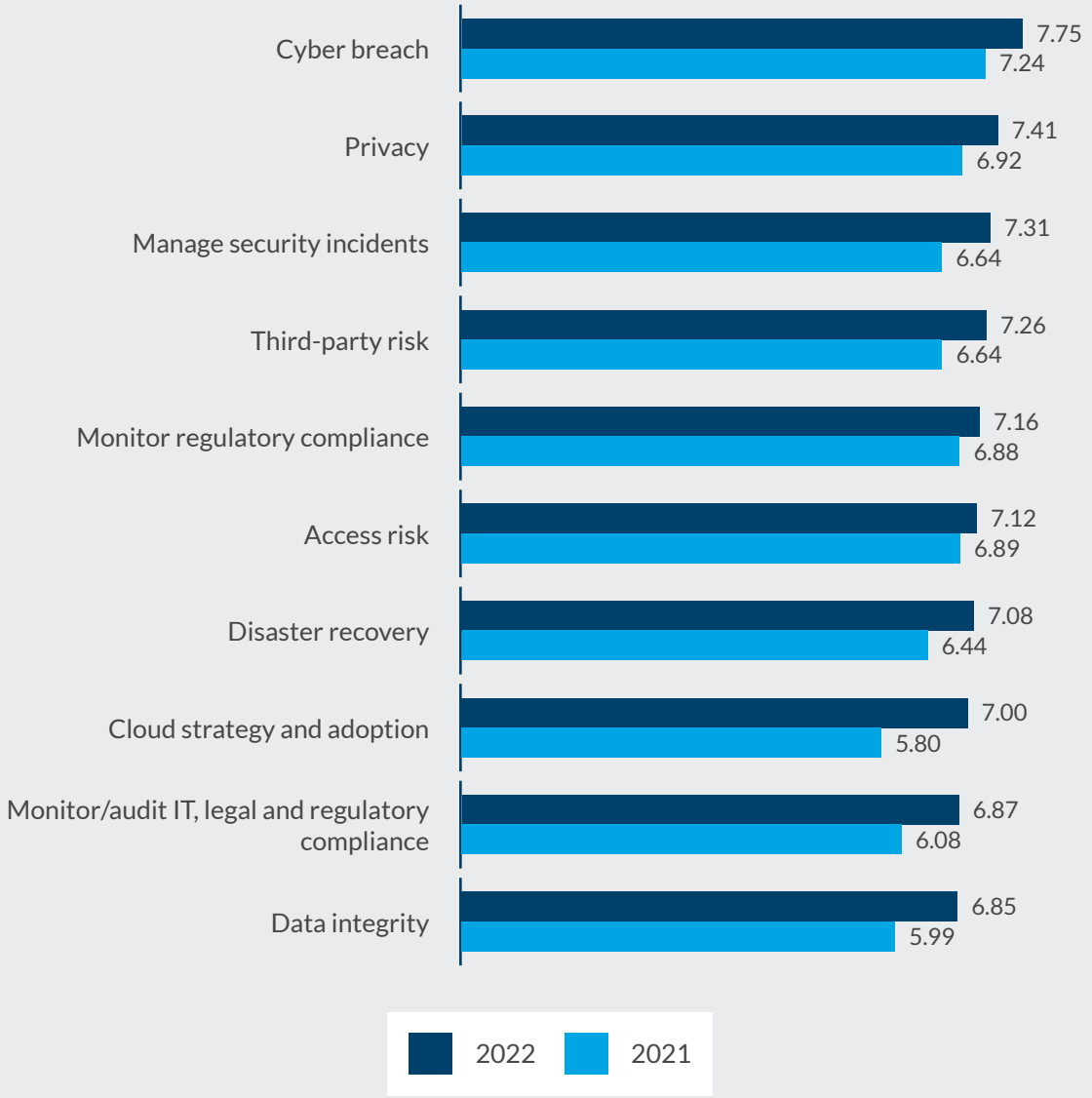
Energy and utilities



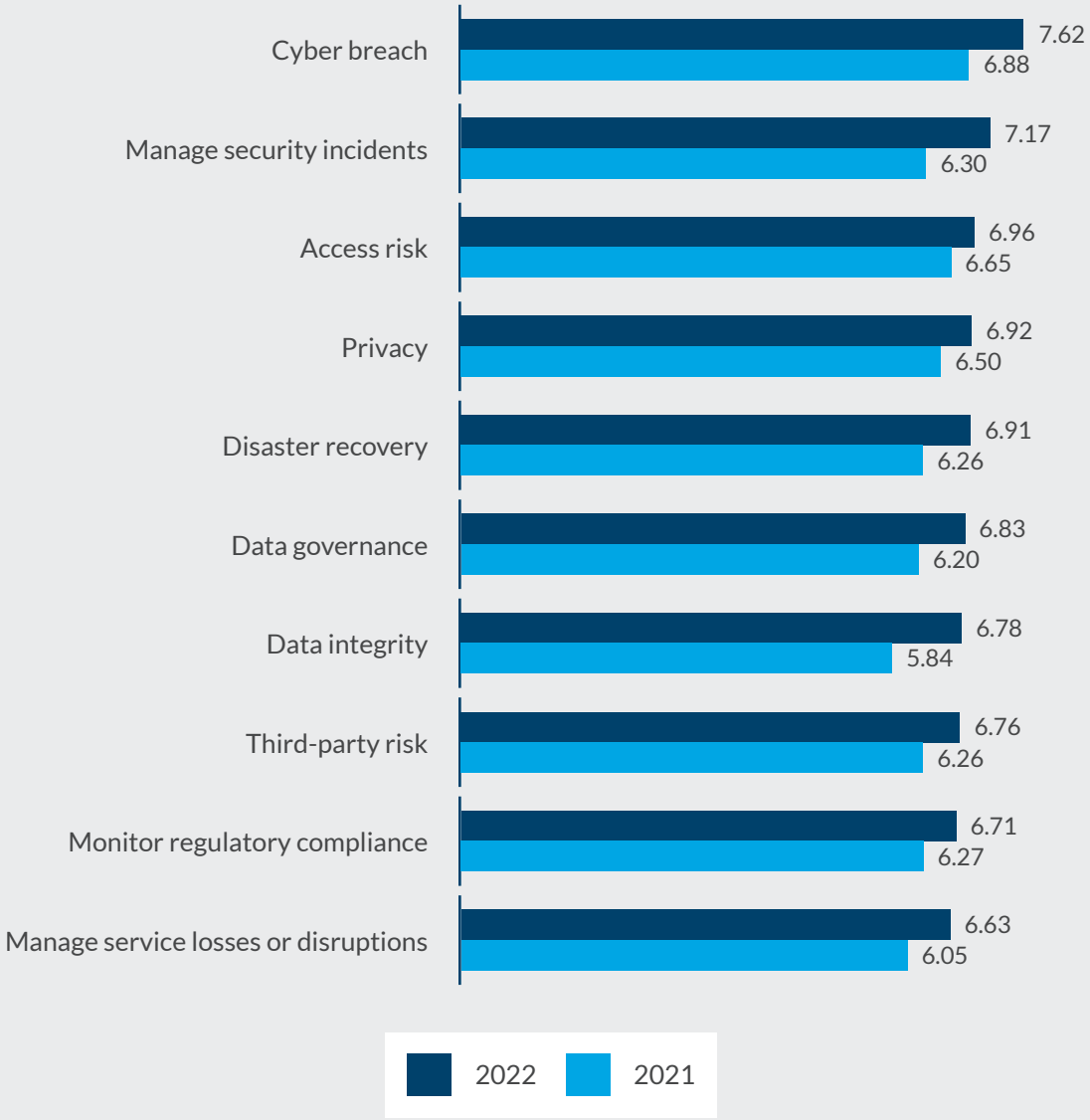
Financial services



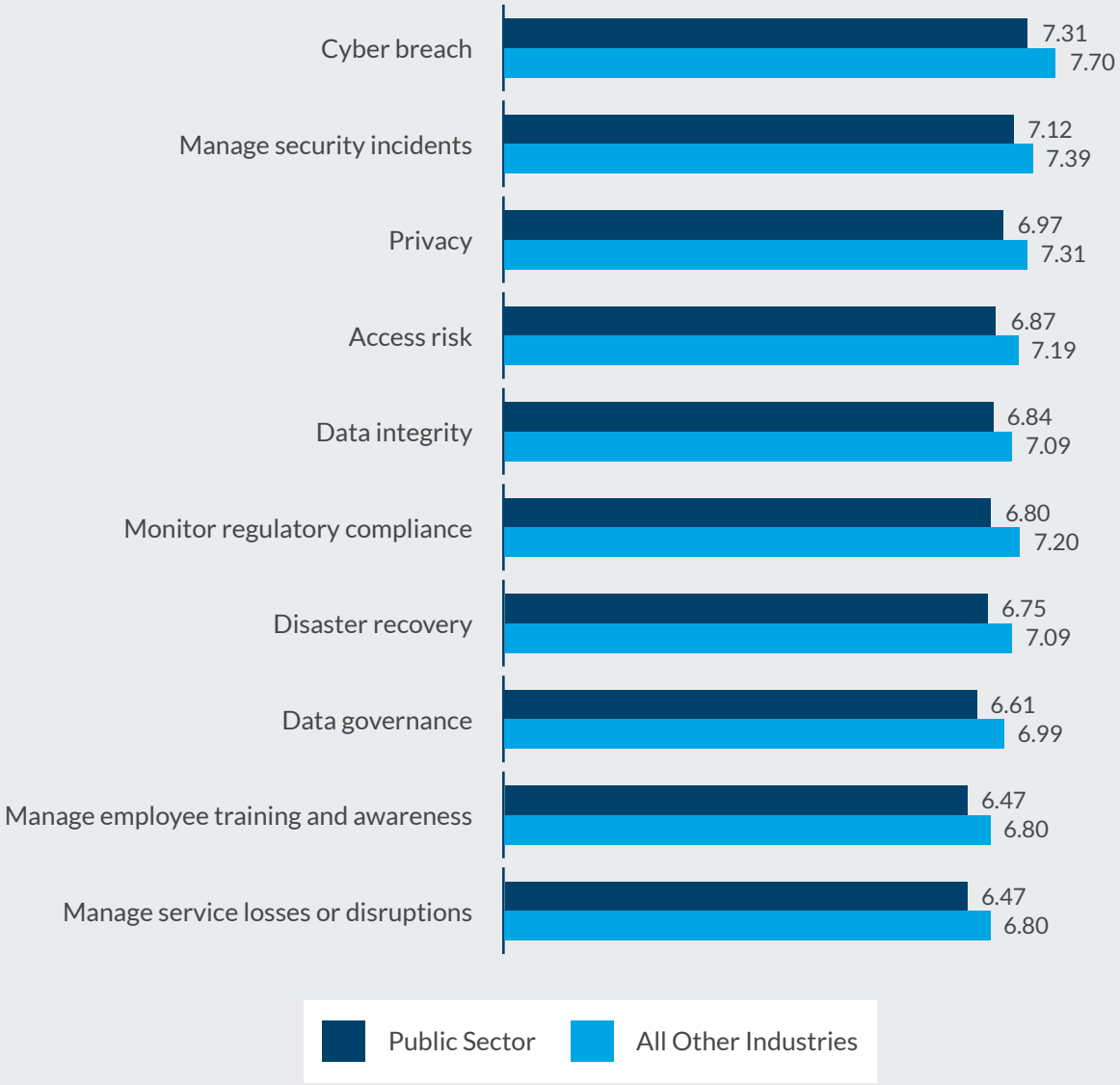
Healthcare


Cyber breach
7.75
7.24
Privacy
7.41
6.92
Manage security incidents
7.31
6.64
Third-party risk
7.26
6.64
Monitor regulatory compliance
7.16
6.88
Access risk
7.12
6.89
Disaster recovery
7.08
6.44
Cloud strategy and adoption
7.00
5.80
Monitor/audit IT, legal and regulatory compliance
6.87
6.08
Data integrity
6.85
5.99
2022
2021

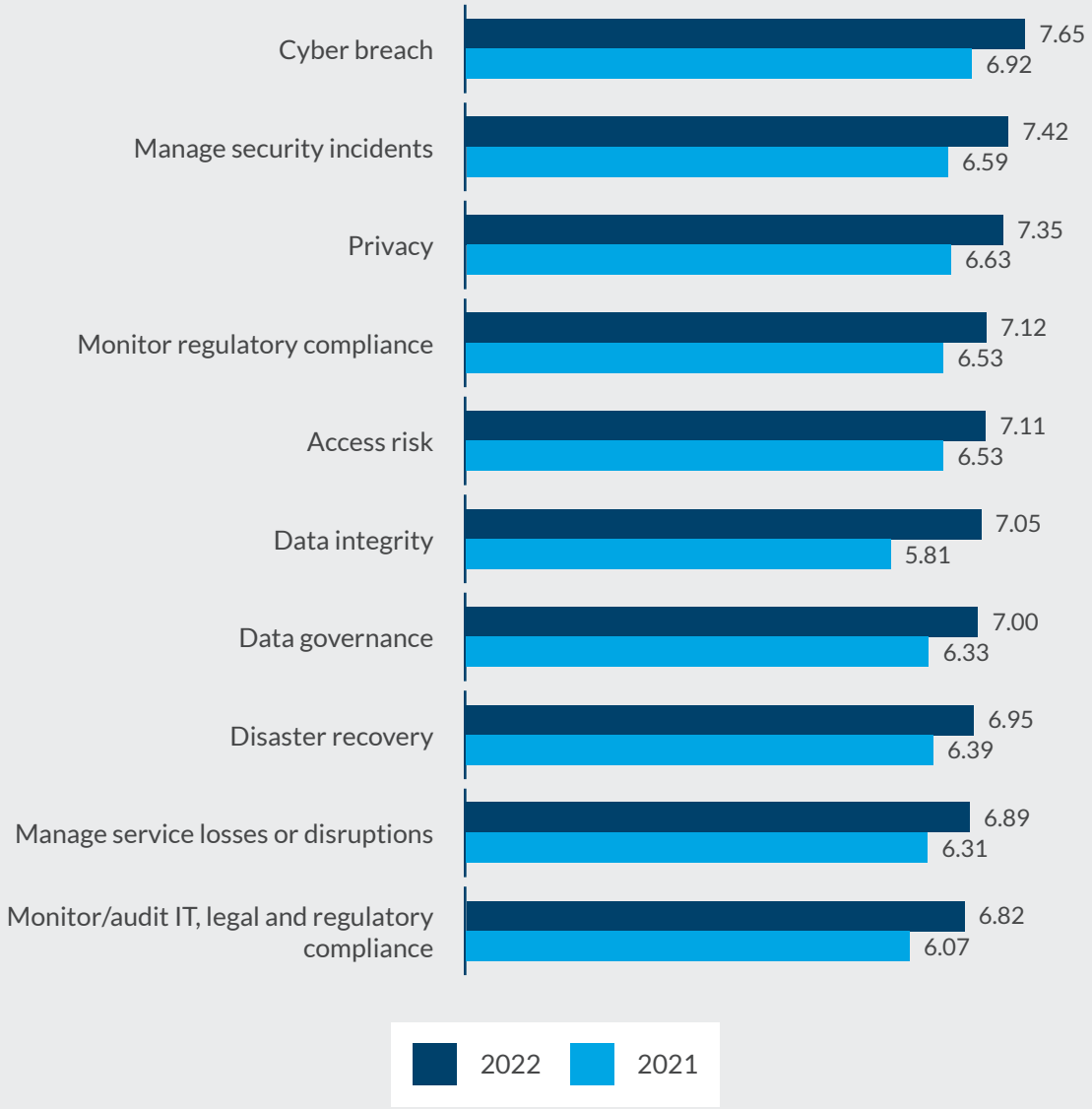
Manufacturing and distribution



Public sector

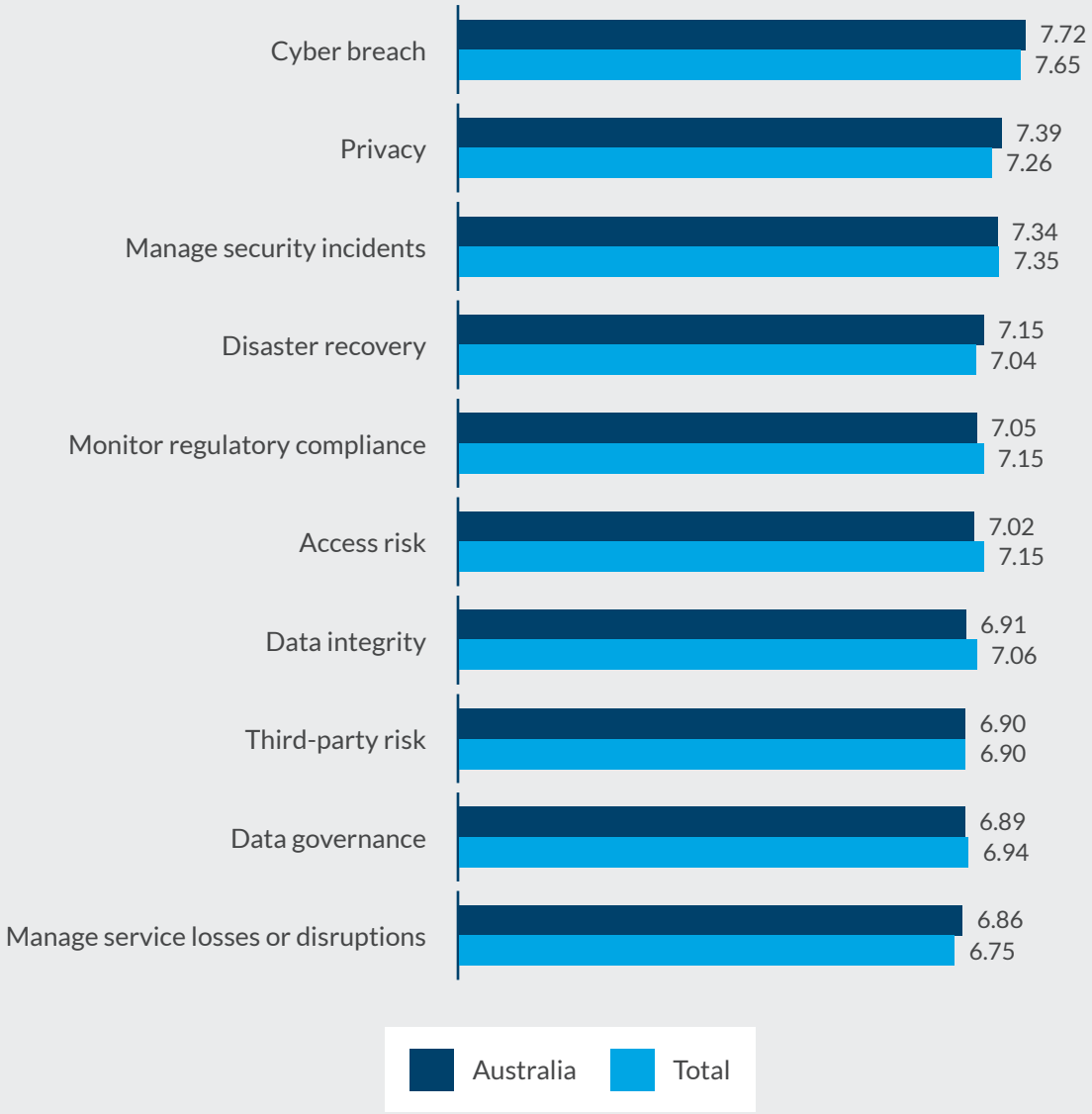


Technology, media and telecommunications

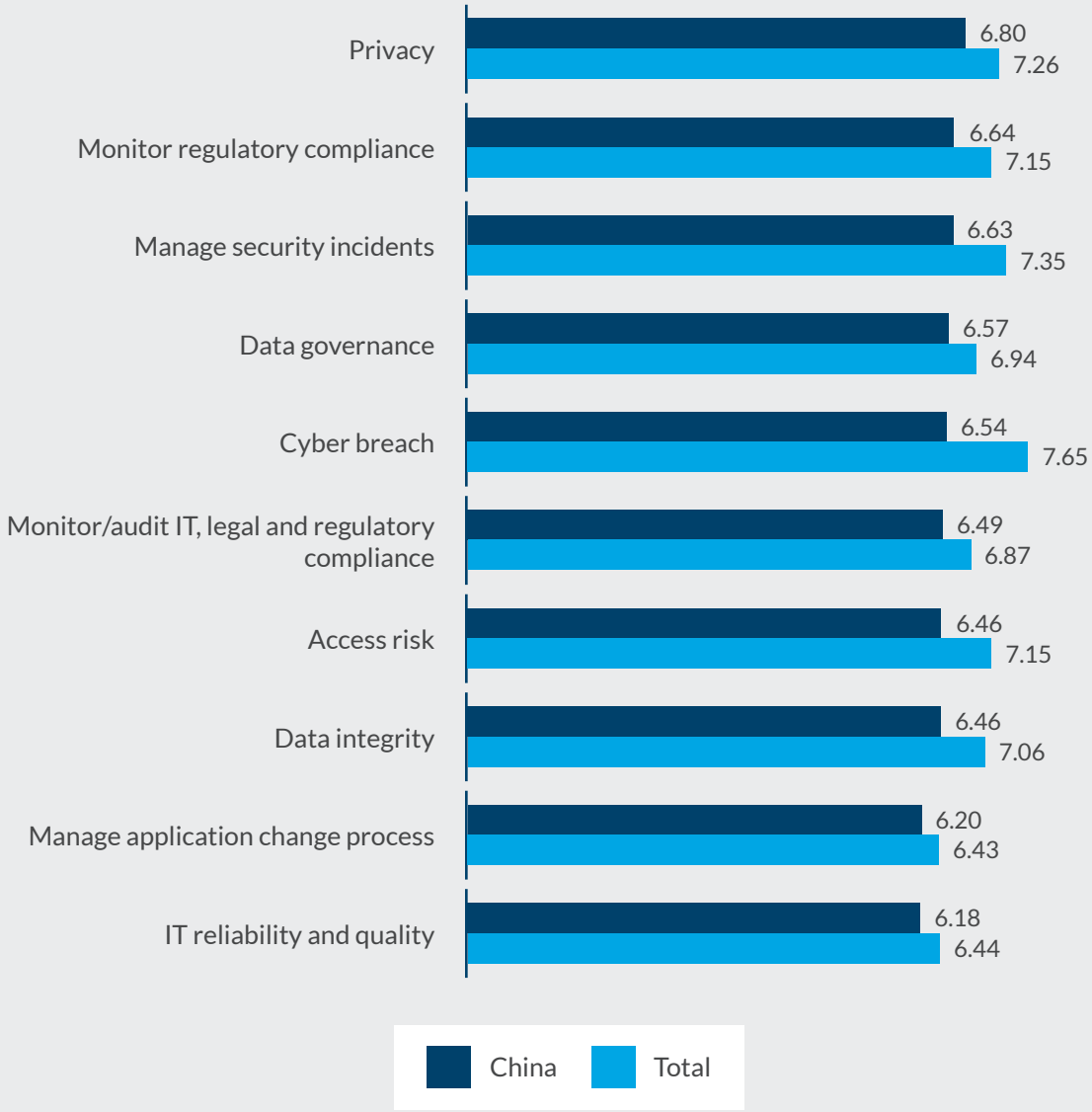


Top 10 technology risk factors by country

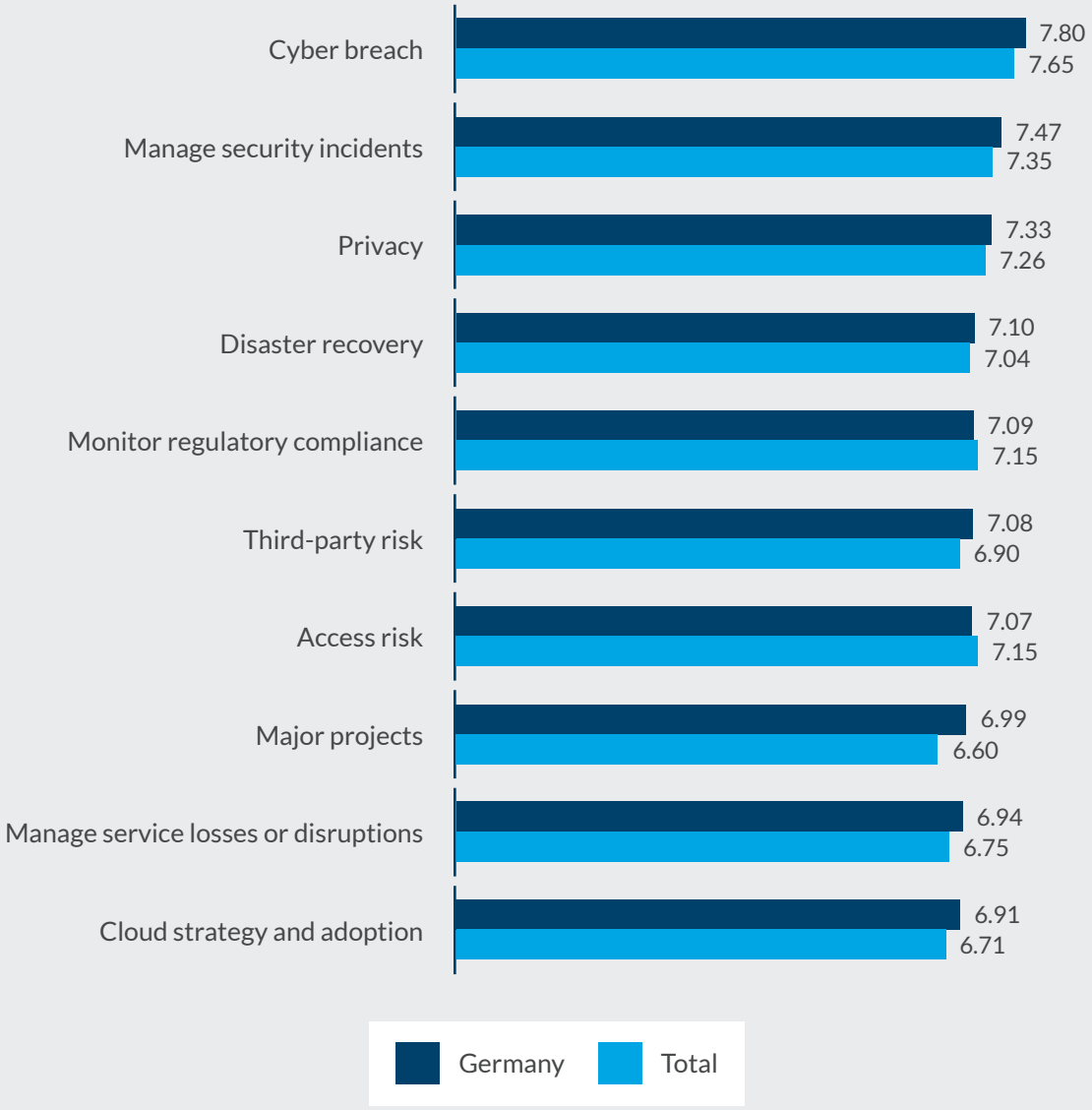
Australia



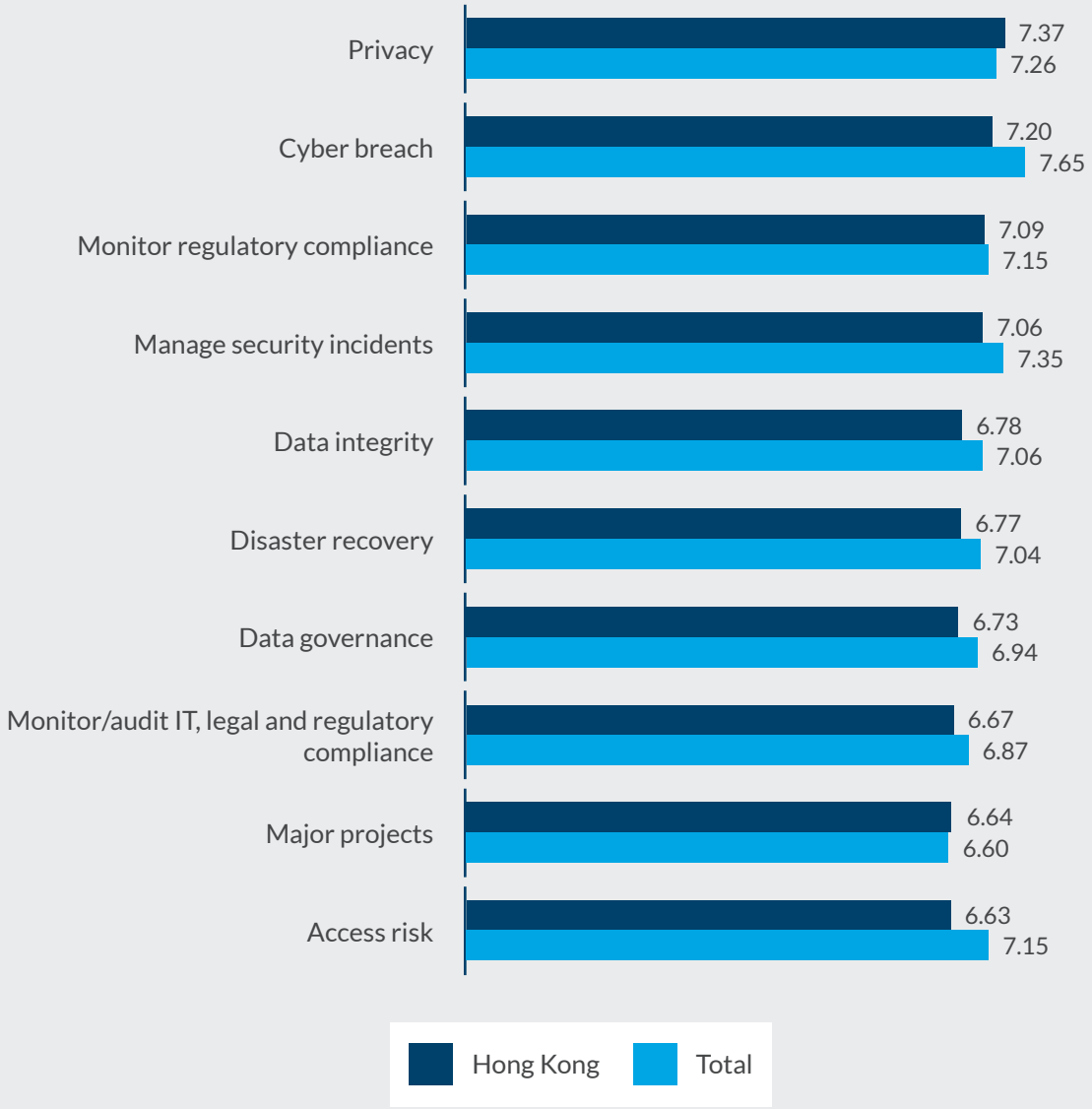
China


Privacy
6.80
7.26
Monitor regulatory compliance
6.64
7.15
Manage security incidents
6.63
7.35
Data governance
6.57
6.94
Cyber breach
6.54
7.65
Monitor/audit IT, legal and regulatory compliance
6.49
6.87
Access risk
6.46
7.15
Data integrity
6.46
7.06
Manage application change process
6.20
6.43
IT reliability and quality
6.18
6.44
China
Total

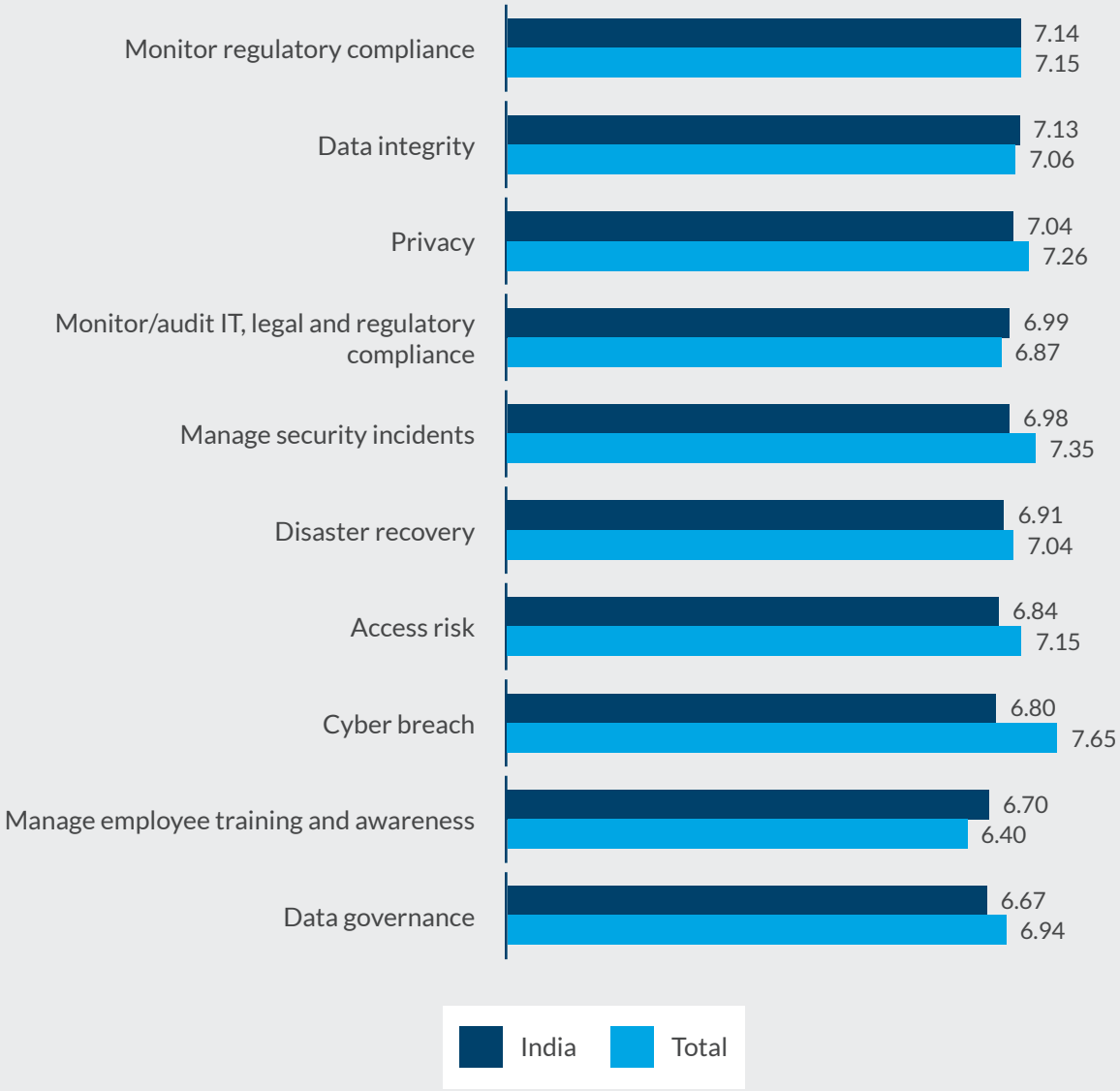
Germany


Cyber breach
7.80
7.65
Manage security incidents
7.47
7.35
Privacy
7.33
7.26
Disaster recovery
7.10
7.04
Monitor regulatory compliance
7.09
7.15
Third-party risk
7.08
6.90
Access risk
7.07
7.15
Major projects
6.99
6.60
Manage service losses or disruptions
6.94
6.75
Cloud strategy and adoption
6.91
6.71
Germany
Total

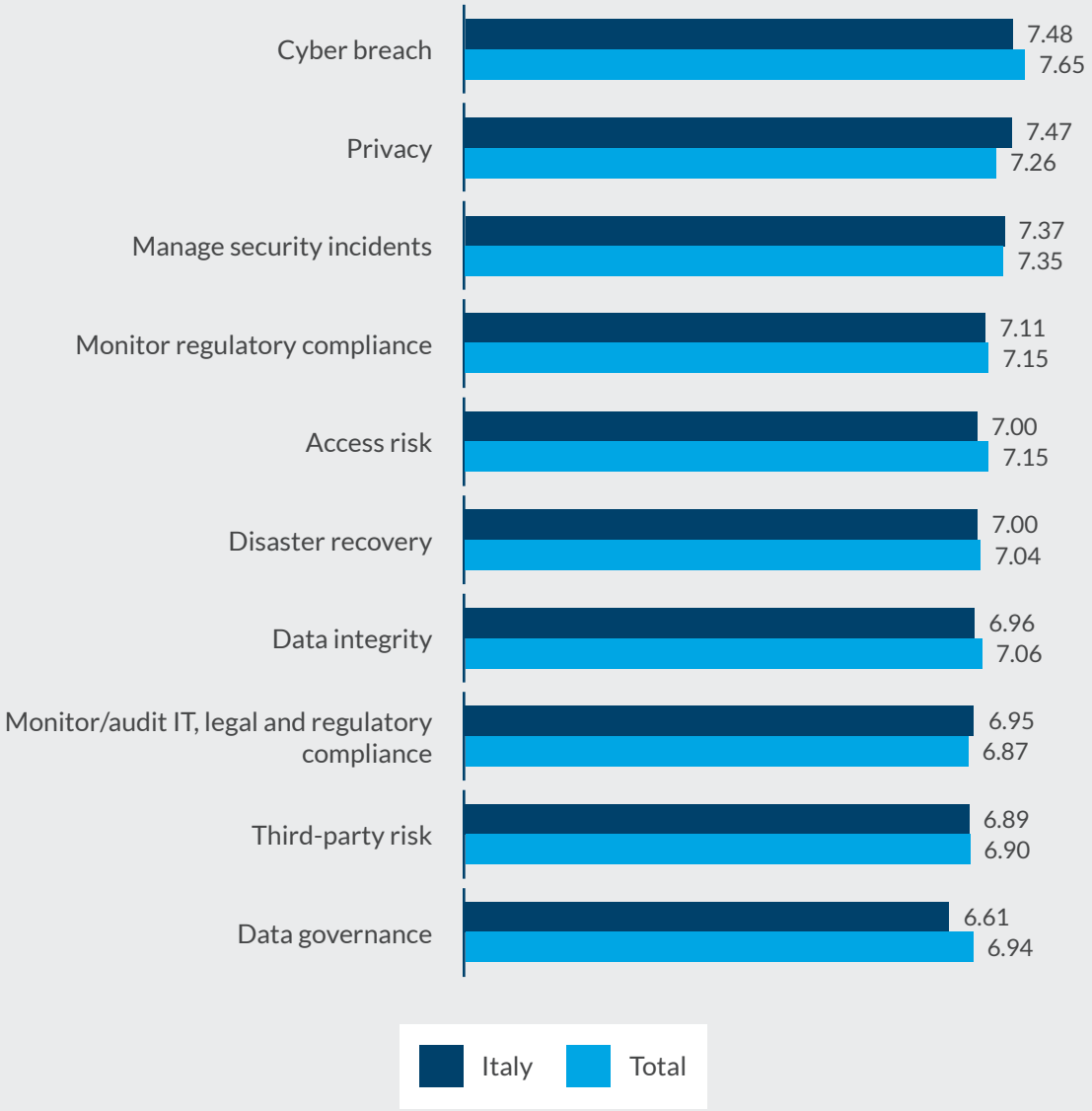
Hong Kong


Privacy
7.37
7.26
Cyber breach
7.20
7.65
Monitor regulatory compliance
7.09
7.15
Manage security incidents
7.06
7.35
Data integrity
6.78
7.06
Disaster recovery
6.77
7.04
Data governance
6.73
6.94
Monitor/audit IT, legal and regulatory compliance
6.67
6.87
Major projects
6.64
6.60
Access risk
6.63
7.15
Hong Kong
Total

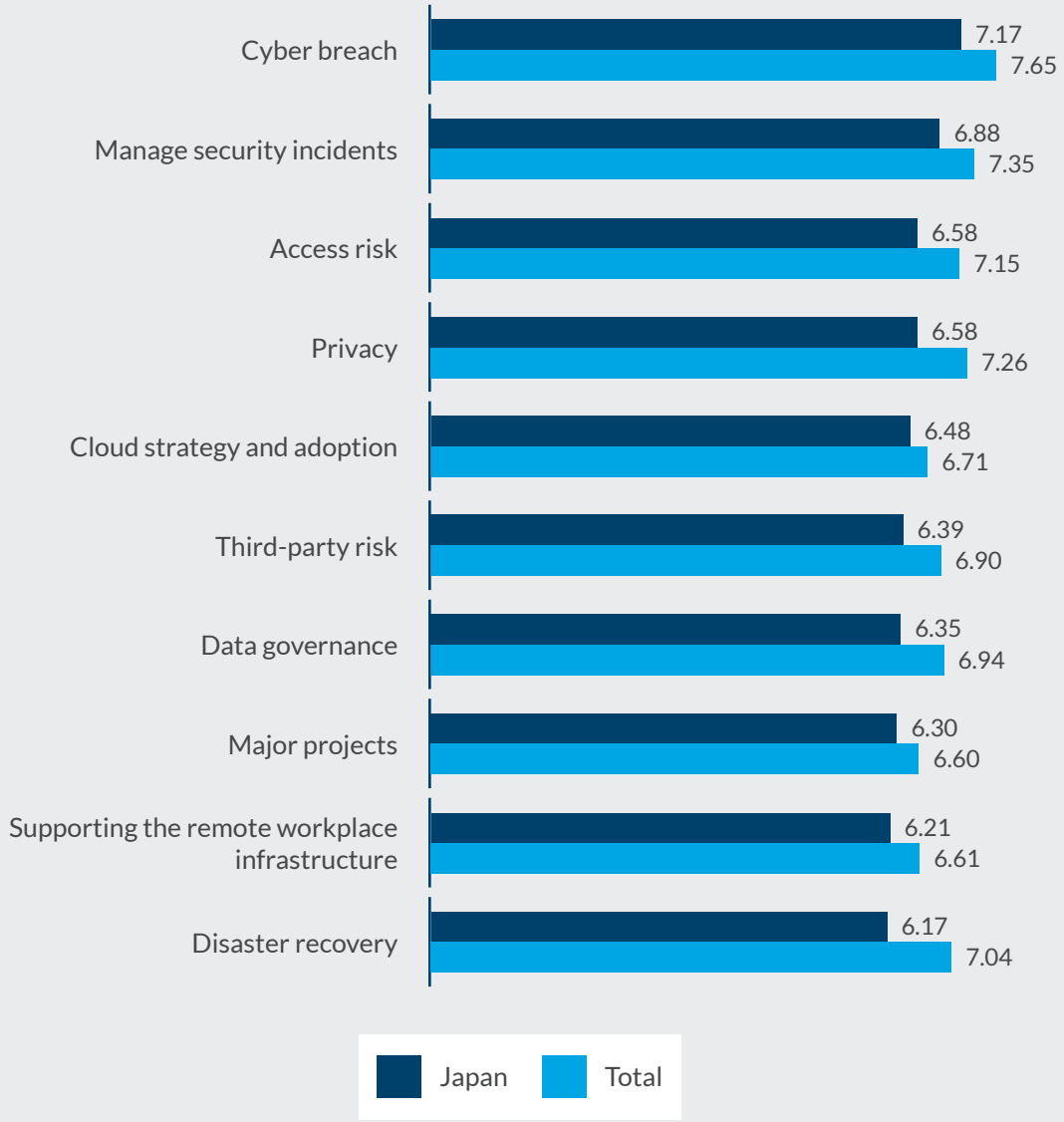
India


Monitor regulatory compliance
7.14
7.15
Data integrity
7.13
7.06
Privacy
7.04
7.26
Monitor/audit IT, legal and regulatory compliance
6.99
6.87
Manage security incidents
6.98
7.35
Disaster recovery
6.91
7.04
Access risk
6.84
7.15
Cyber breach
6.80
7.65
Manage employee training and awareness
6.70
6.40
Data governance
6.67
6.94
India
Total

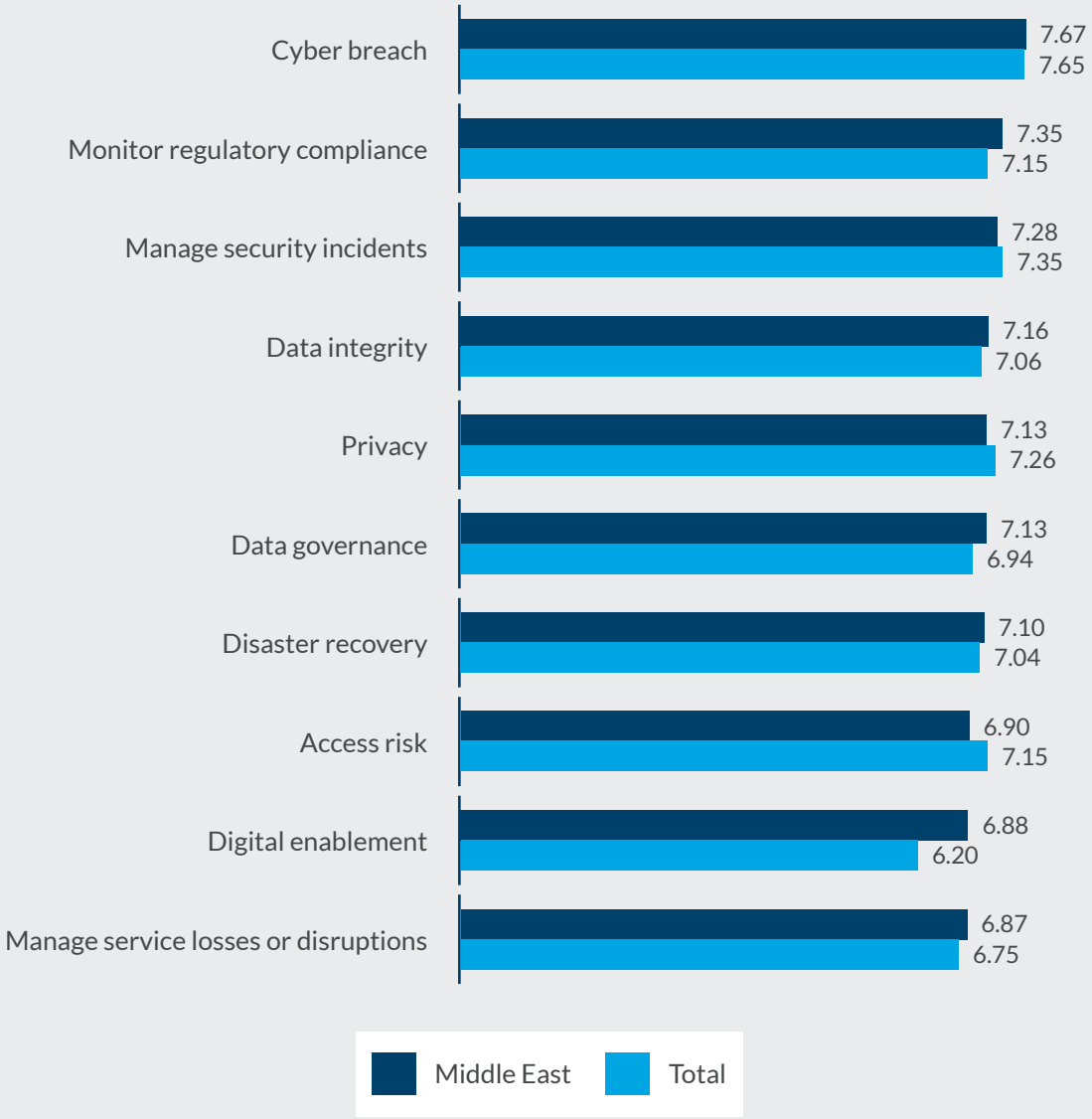
Italy


Cyber breach
7.48
7.65
Privacy
7.47
7.26
Manage security incidents
7.37
7.35
Monitor regulatory compliance
7.11
7.15
Access risk
7.00
7.15
Disaster recovery
7.00
7.04
Data integrity
6.96
7.06
Monitor/audit IT, legal and regulatory compliance
6.95
6.87
Third-party risk
6.89
6.90
Data governance
6.61
6.94
Italy
Total

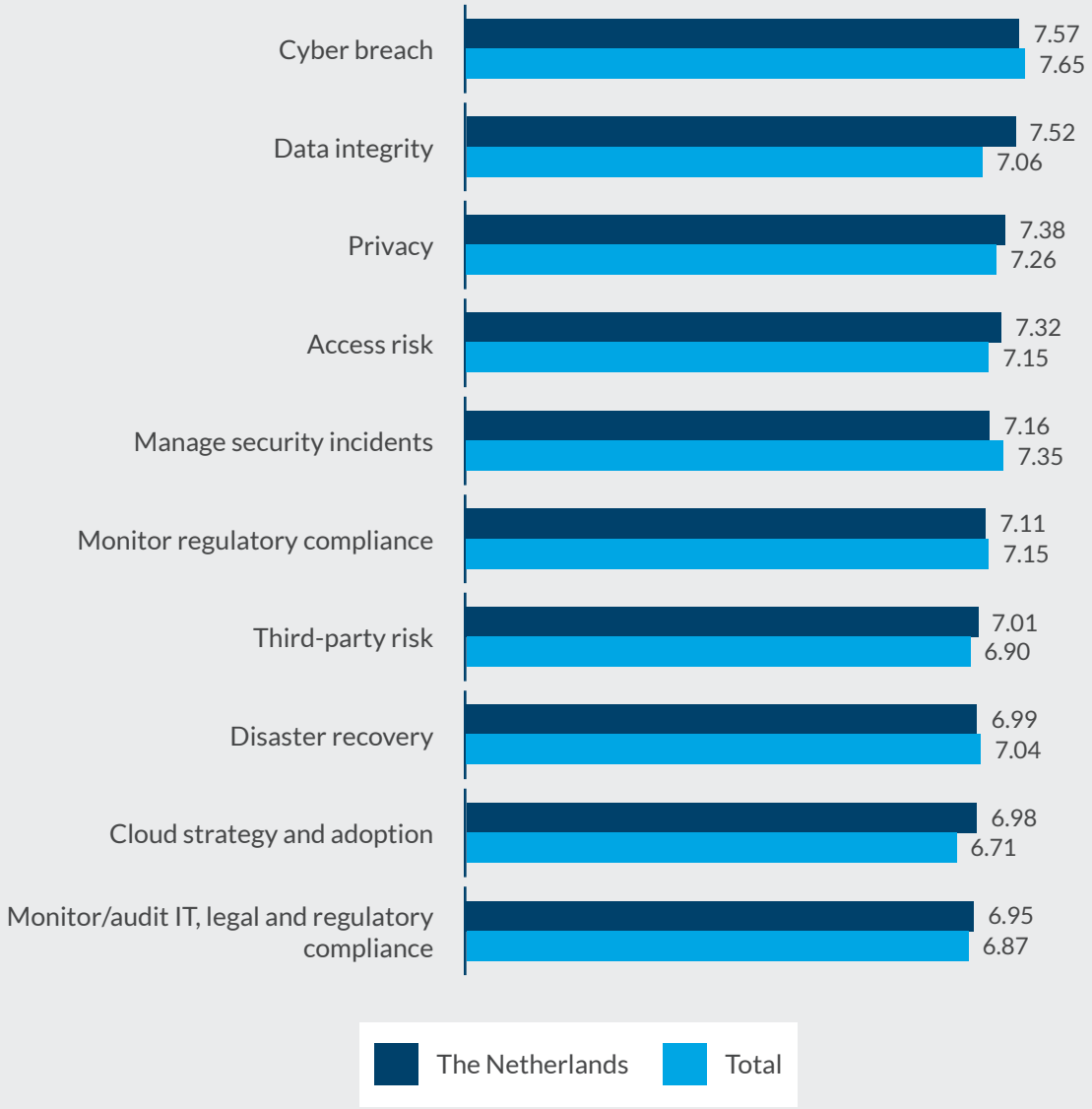
Japan


Cyber breach
7.17
7.65
Manage security incidents
6.88
7.35
Access risk
6.58
7.15
Privacy
6.58
7.26
Cloud strategy and adoption
6.48
6.71
Third-party risk
6.39
6.90
Data governance
6.35
6.94
Major projects
6.30
6.60
Supporting the remote workplace infrastructure
6.21
6.61
Disaster recovery
6.17
7.04
Japan
Total

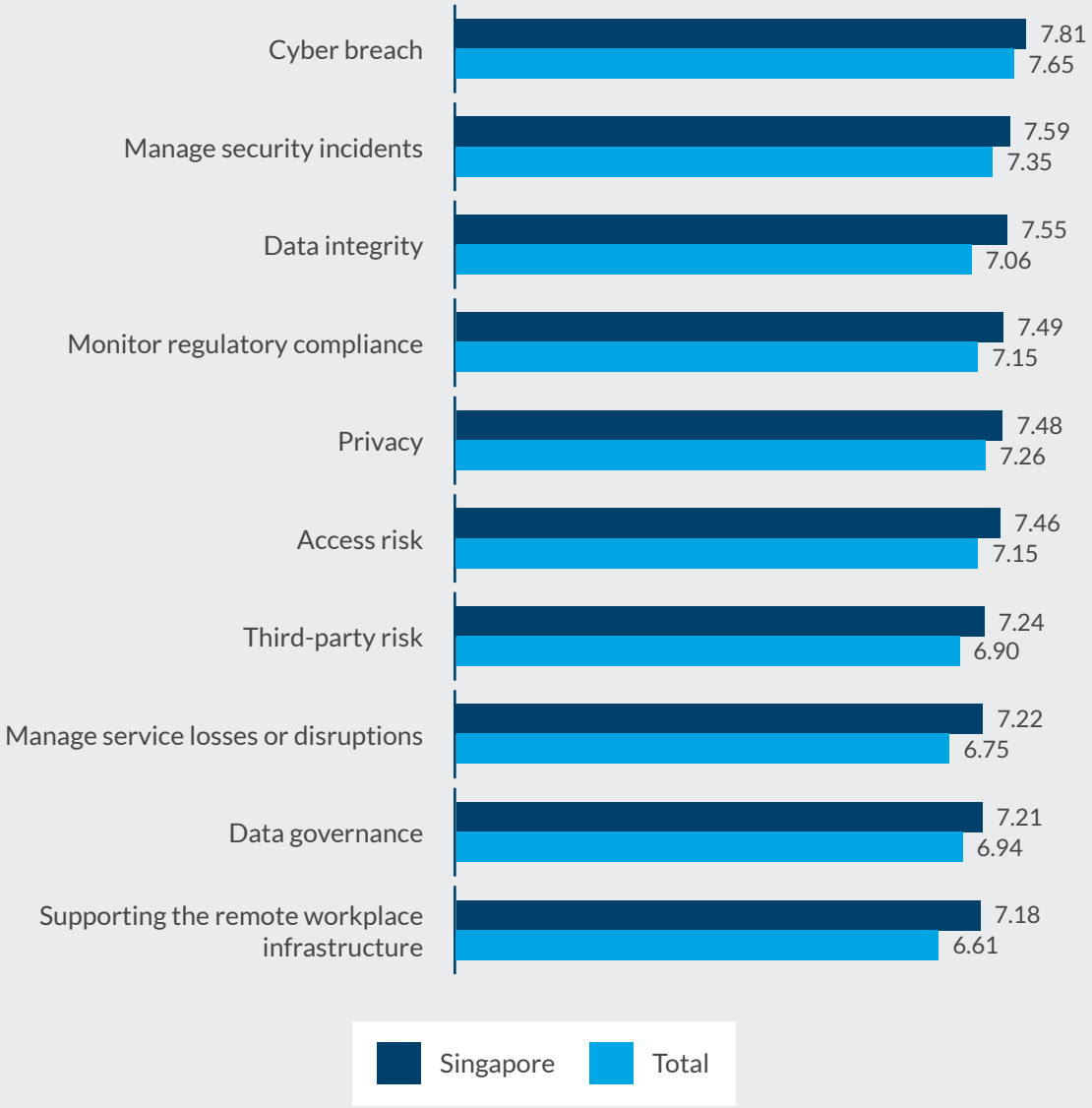
Middle East


Cyber breach
7.67
7.65
Monitor regulatory compliance
7.35
7.15
Manage security incidents
7.28
7.35
Data integrity
7.16
7.06
Privacy
7.13
7.26
Data governance
7.13
6.94
Disaster recovery
7.10
7.04
Access risk
6.90
7.15
Digital enablement
6.88
6.20
Manage service losses or disruptions
6.87
6.75
Middle East
Total

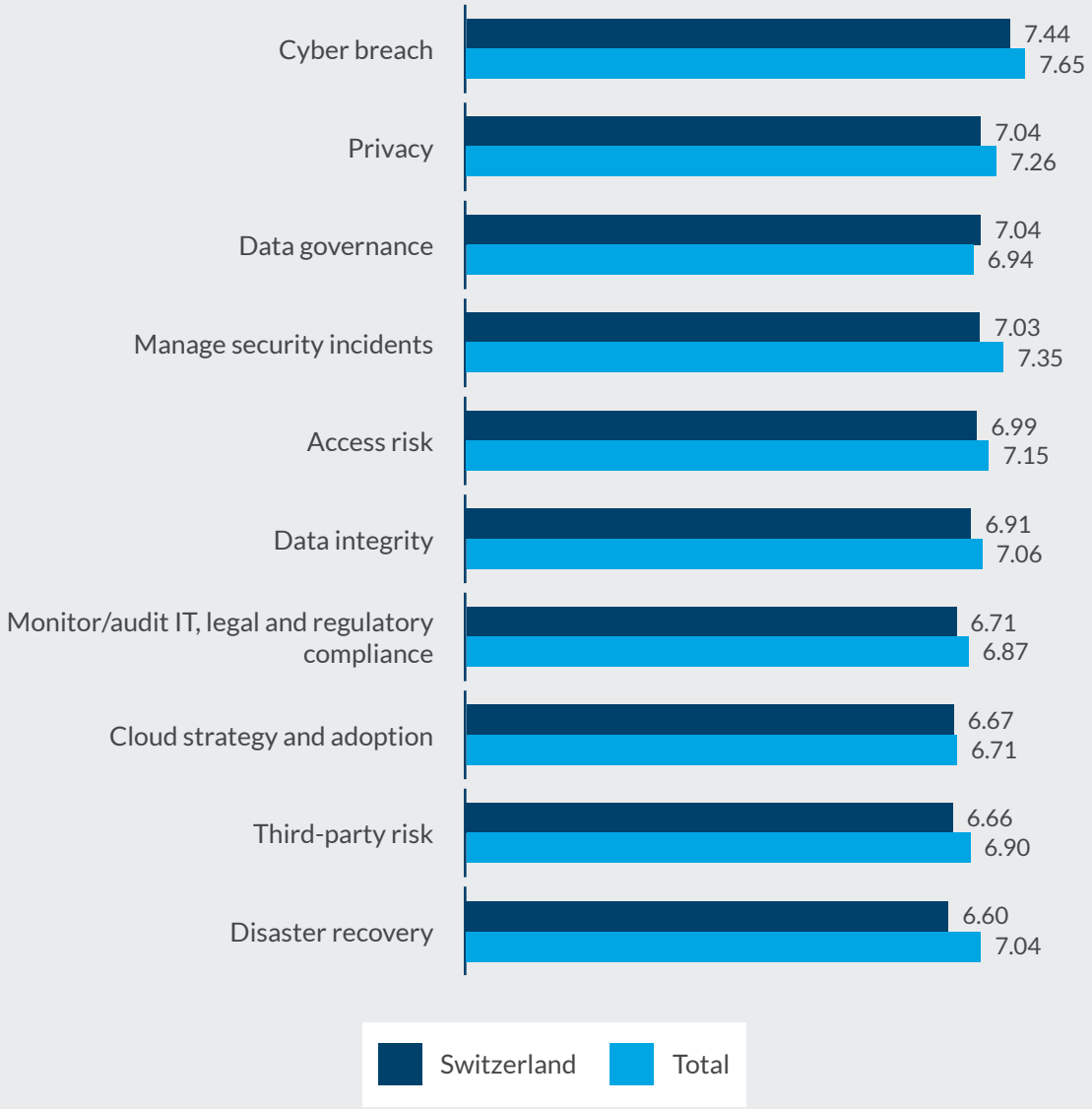
The Netherlands



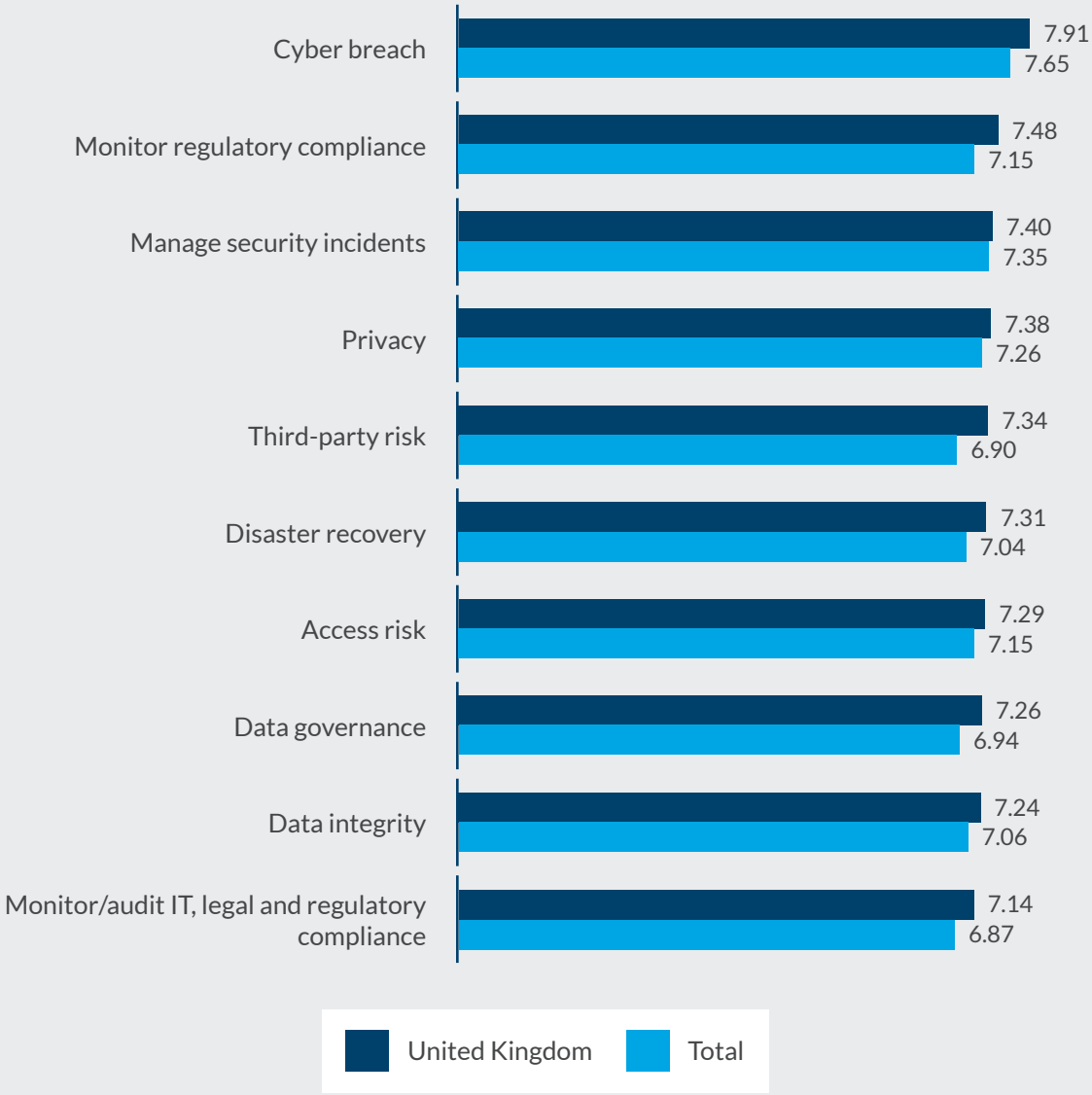
Singapore


Cyber breach
7.81
7.65
Manage security incidents
7.59
7.35
Data integrity
7.55
7.06
Monitor regulatory compliance
7.49
7.15
Privacy
7.48
7.26
Access risk
7.46
7.15
Third-party risk
7.24
6.90
Manage service losses or disruptions
7.22
6.75
Data governance
7.21
6.94
Supporting the remote workplace infrastructure
7.18
6.61
Singapore
Total

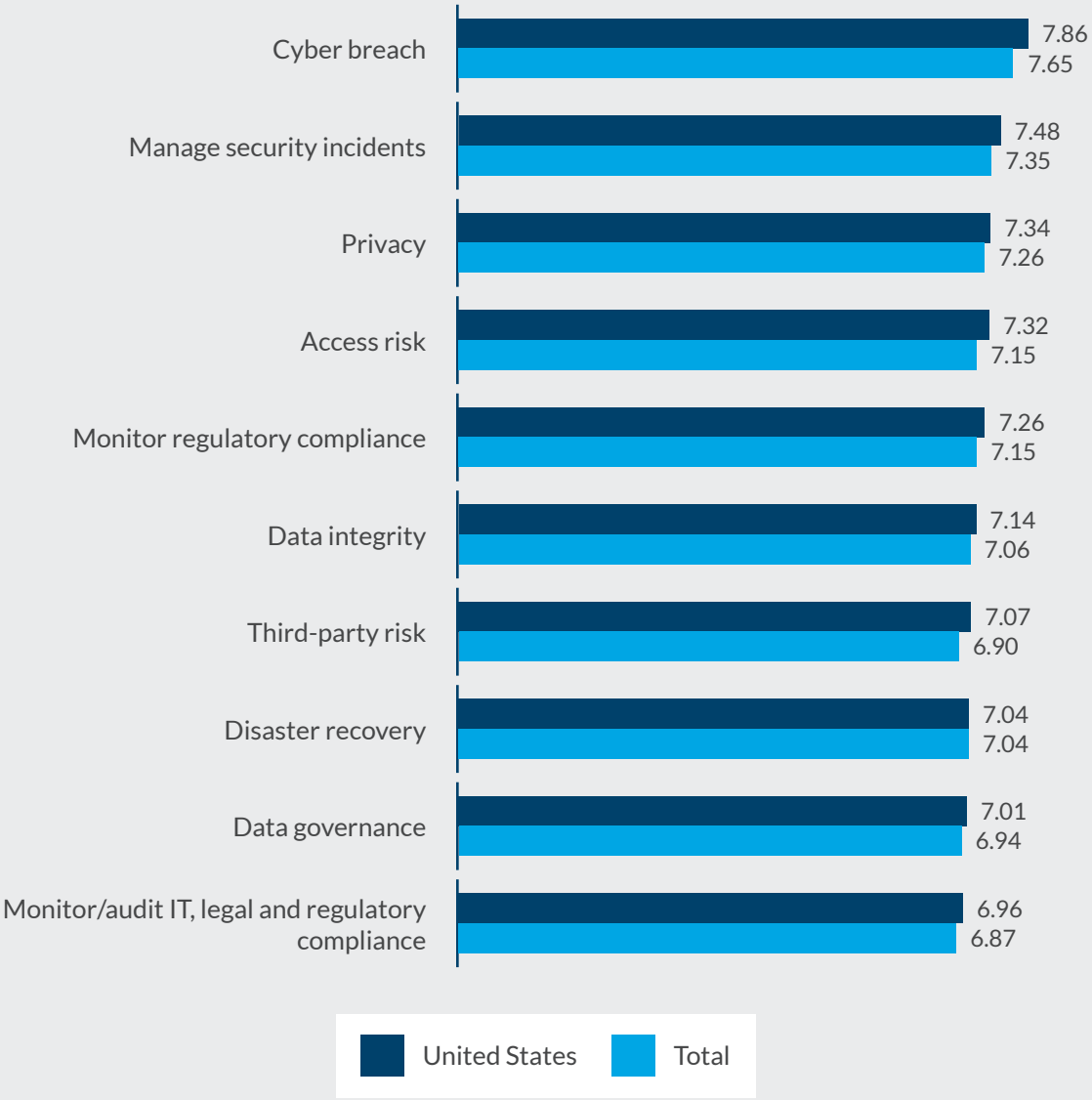
Switzerland



United Kingdom



United States



Assessing technology audit risk management practices

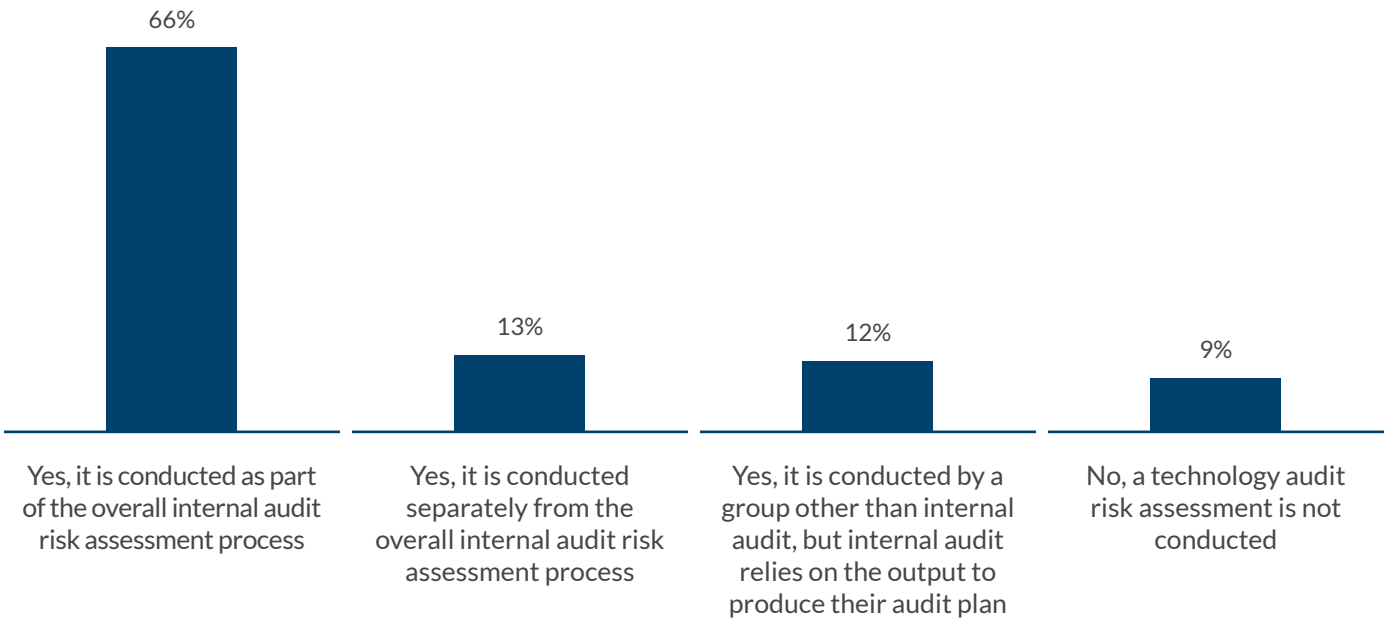
Our research findings on technology audit risk management approaches — including how frequently technology risk is evaluated and the factors that trigger changes to technology risk assessments among similar processes — highlight some of the starkest differences between leading and lagging IT audit functions, based on the overall maturity of the function, depth of experience, certifications and peer review processes, among other factors.

It is encouraging that more than nine in 10 responding organisations assess technology risk for planning purposes. It is also noteworthy that more than three-quarters of IT audit teams that conduct these assessments as part of the internal audit risk assessment process do so on a monthly or more frequent basis. This approach contrasts markedly with the 9% of respondents whose IT audit teams do not assess technology risk for audit planning purposes at all, let alone on a monthly or periodic basis.

Organisations that include technology risk assessments in their annual plans employ a range of methods for doing so, the most common of which involves the integration of technology risk assessments into the overall internal audit risk assessment process. Others conduct the technology risk assessment separately from the overall internal audit risk assessment process, while in some organisations it is conducted by a group other than internal audit, but internal audit relies on the output to produce the audit plan.

Regardless of which method is used, it is imperative to assess technology risk, and it has become prudent to do so as frequently as possible from a practical standpoint. Our results show that one-third of IT audit functions conduct these assessments monthly or more frequently. This vigilance reflects a risk-savvy approach to assessing the dynamic technology environments both inside and outside the organisation.

Does your organisation assess technology risk for audit planning purposes?

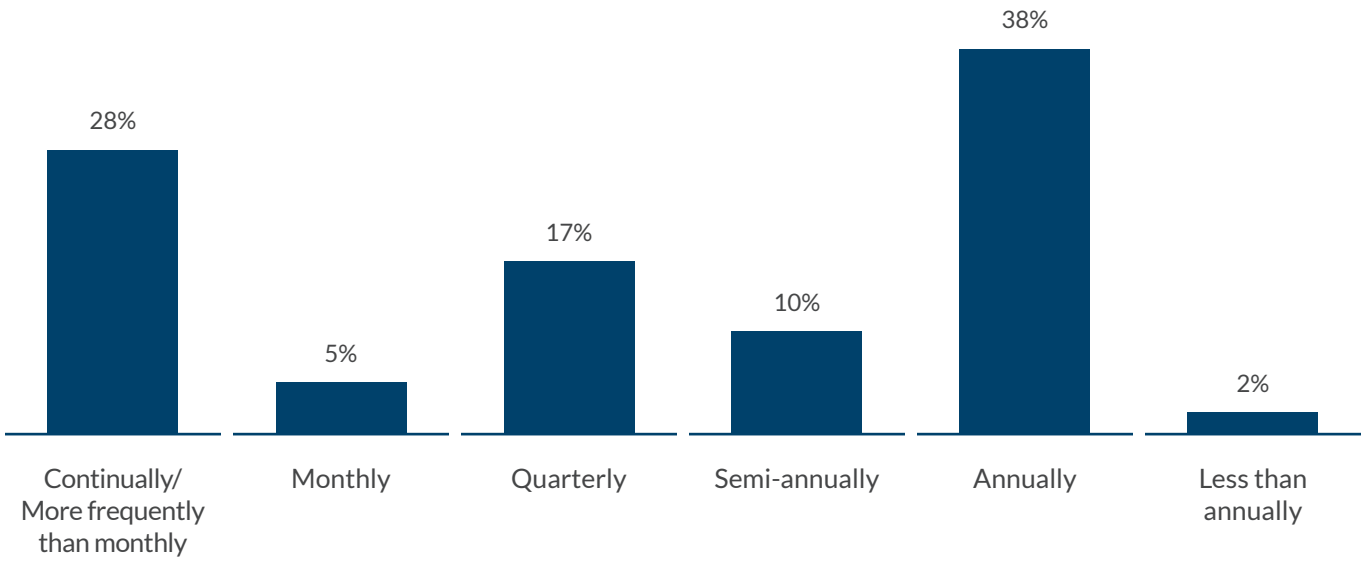


In considering options for performing technology risk assessments more frequently, a new and expanding crop of technology tools and applications can equip IT audit teams with valuable support in automating many of the manual tasks associated with assessing and continually monitoring technology risk. The availability of these supporting technologies, combined with the rapidly changing technology risk landscape, should challenge IT audit leaders in organisations that currently assess technology risk once a year or even less frequently to ask: *What talent, skills and tools do we need to enable us to conduct these assessments on a quarterly, monthly or even more frequent basis?*

The ability to adjust the nature and frequency of technology risk assessments in response to changing business conditions and the emergence of new risk concerns represents another notable difference between more mature and less mature IT audit capabilities. Many organisations recalibrate their technology audit assessment processes not only in the face of increased risk impact and likelihood, but also in response to shifts in persistence (the potential duration of the risk event) and/or velocity (the potential speed at which a risk event materialises). However, a majority of IT audit groups have yet to adapt their risk assessment processes in response to persistence and velocity; as such, they should consider how to incorporate these factors into their assessment capabilities.

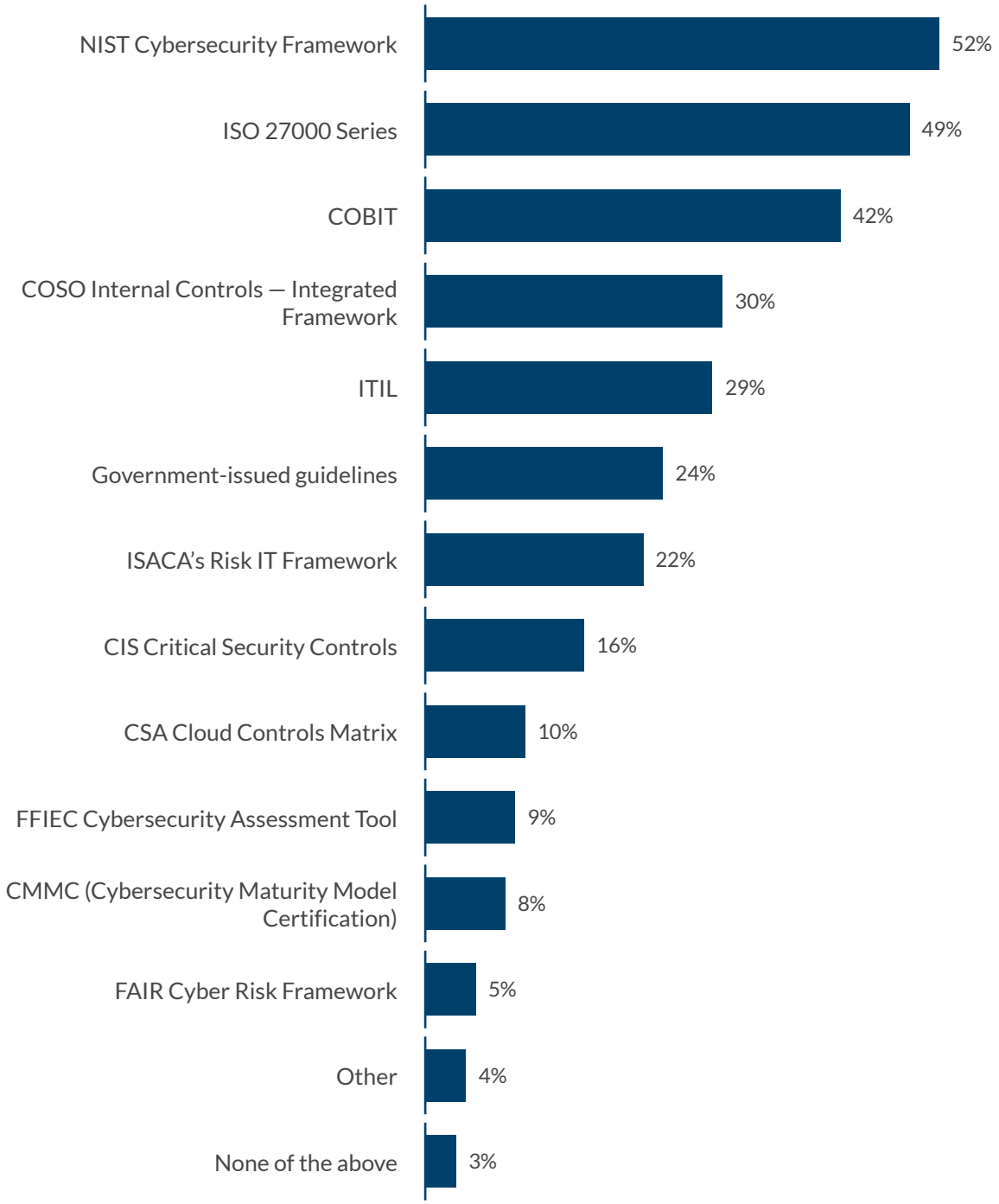
If further motivation is needed on this count, consider that four in 10 organisations did not adjust the nature or frequency of their technology risk assessments in response to COVID-related disruption and related changes to business conditions (e.g., remote work, war-related sanctions compliance and new cybersecurity requirements from global authorities). This inaction pervades despite the fact that more than 60% of organisations report that new models of work deployed in response to the pandemic have had a moderate to significant impact on technology risk.

How often does the process to assess technology risk occur within the organisation?*



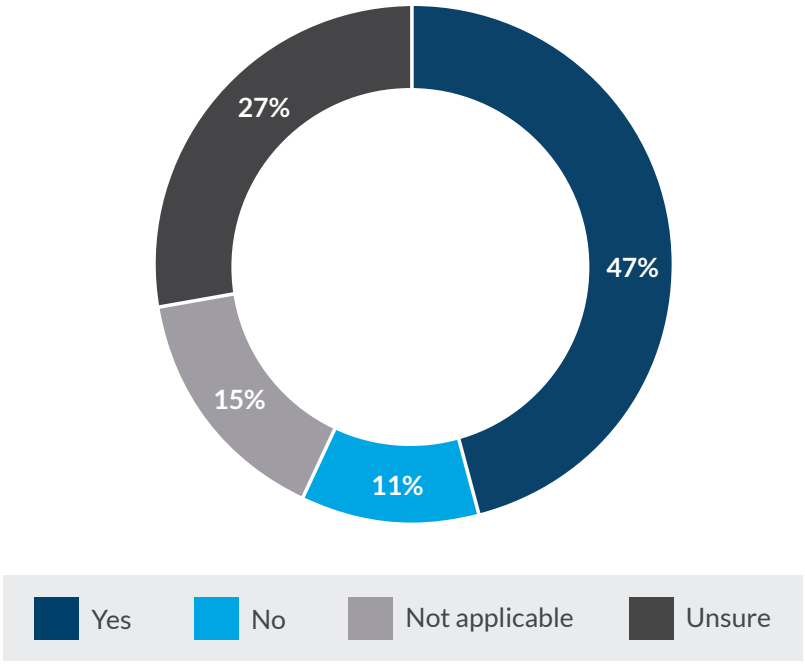
* Base: Among organisations that assess technology risk for audit planning purposes.

• • • On which of the following accepted industry framework(s) is the process to identify and assess technology risk based?* (Multiple responses permitted.)

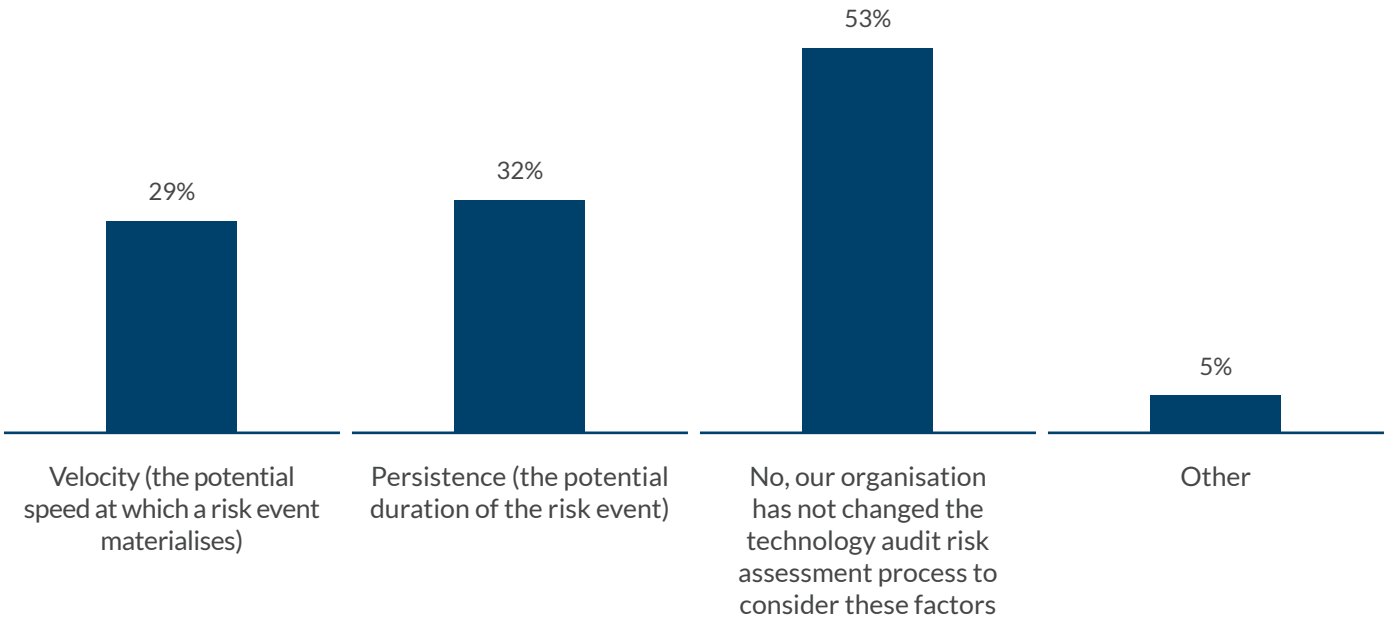


* Base: Among organisations that assess technology risk for audit planning purposes.

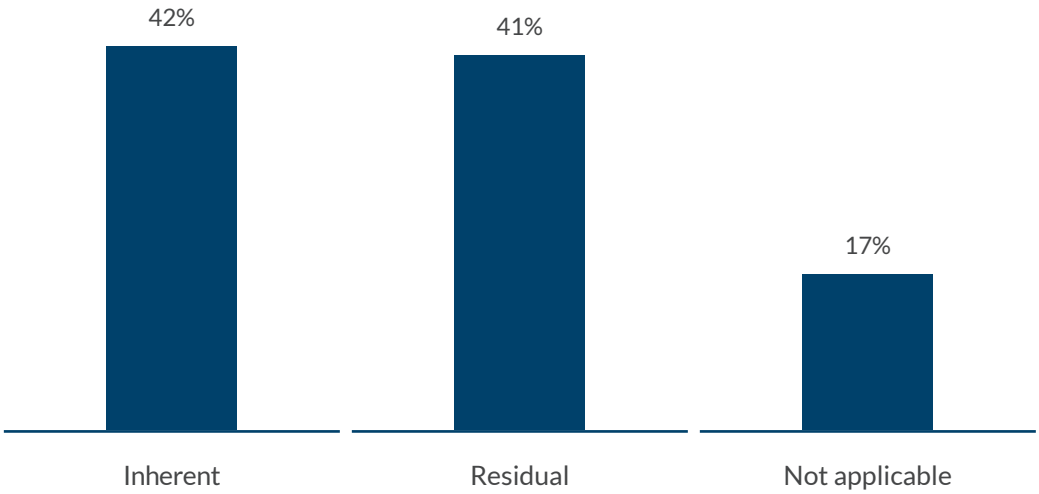
If your company has an ERM (or technology risk) programme, does the technology audit risk framework used for the risk assessment align with or link to the ERM (or technology risk) framework?



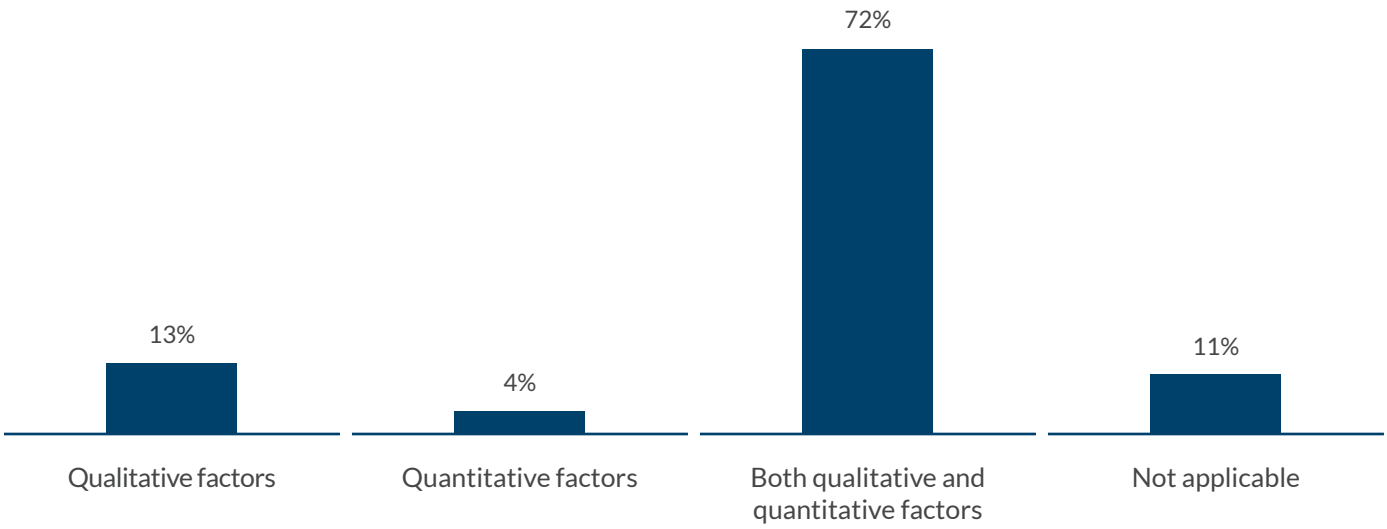
Has your organisation changed the technology audit risk assessment process to consider any of the following factors, beyond impact and likelihood? (Multiple responses permitted.)



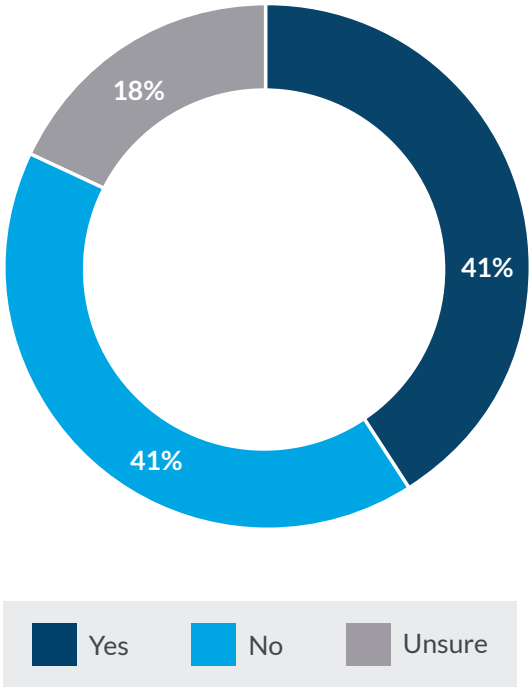
How does the technology audit risk assessment evaluate risk?



How are technology risks evaluated through the technology audit risk assessment process?



• • • **Have COVID-related disruptions and related changes to business conditions caused you to adjust the nature or frequency of technology risk assessments?**



Rethinking the office

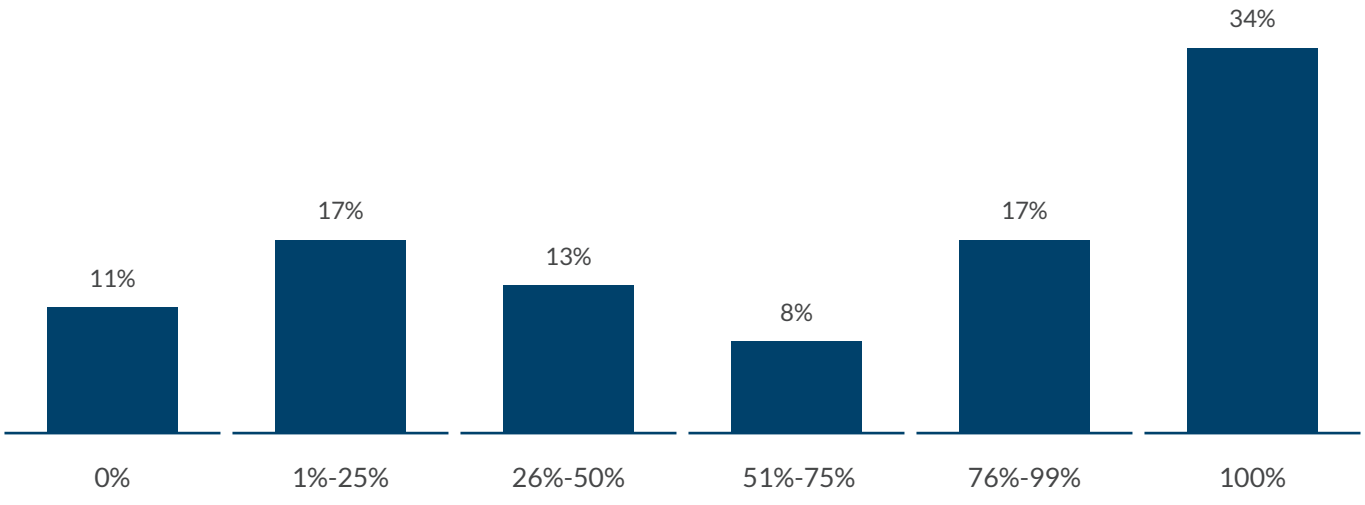
Like other parts of the organisation, many IT audit teams transitioned to remote working models in the past two years and many expect to work remotely on a full-time basis moving forward. It is promising that a relatively small portion of organisations report that the IT audit group's productivity declined while engaging in varying levels of remote work over the past year. And while IT audit leaders have amassed valuable insights and knowledge from the pandemic-driven shift to remote and hybrid working models, caution is warranted.

Making a longer-term transition to remote or hybrid working models requires much more than equipping IT auditors with a laptop, secure high-speed connectivity and access to a video platform. For IT audit as well as any function in the organisation, there are broader and deeper considerations around collaboration, connectivity (of the human variety) and culture. It is important to keep in mind that playbooks for hybrid working models remain in draft form — and must be tailored to support the unique needs and characteristics of each organisation and, oftentimes, different functional and operations groups within the same enterprise.

While many IT audit teams transitioned to remote work and hybrid work better than anyone could have imagined, it's time to leverage those learnings and insights by addressing more strategic questions about the future of work, offices, and the labour models that IT audit leaders, and their colleagues, use to build long-term value for the organisation.[6]

The survey results also confirm the need for bigger-picture thinking concerning the talent and skills IT audit leaders need to attract, engage, retain and develop. Fifteen percent of IT audit leaders and professionals are concerned about a lack of access to IT audit talent and skills, yet most also report that they are relying heavily on traditional modes of addressing this need (training and developing as well as hiring) amid what projects to be a deep and long-term technology talent shortage. Further, less than half report that senior management and board committees support IT audit groups in their increasingly challenging efforts to acquire or develop the talent and skills they need to thrive.

What percentage of your IT audit team is currently working remotely on a full-time basis?



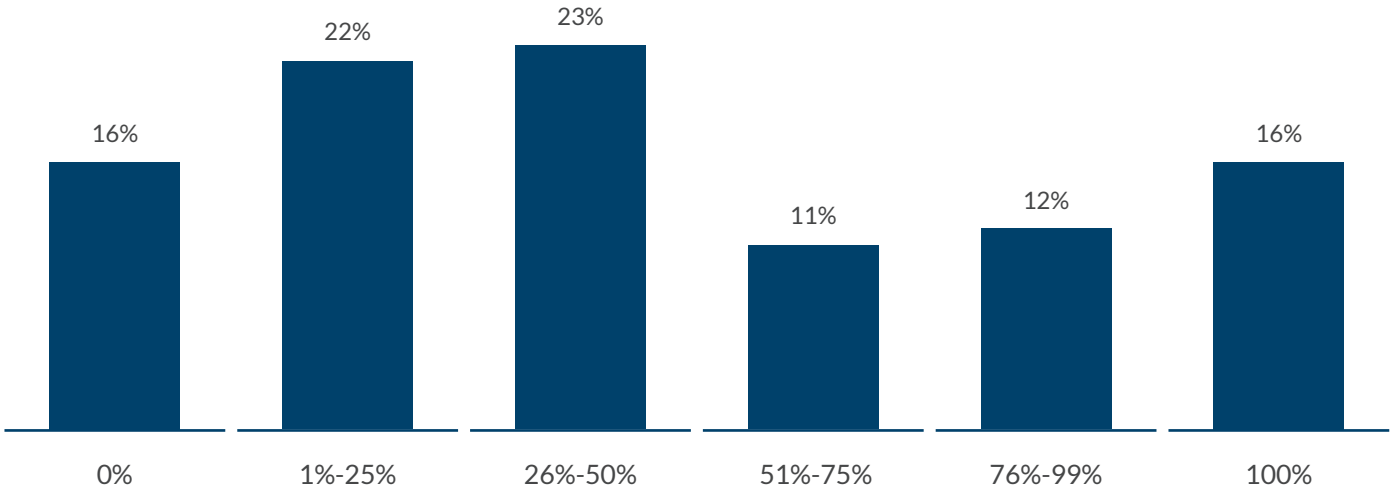
[6] "Performance Over Presence: Rethinking the Post-Pandemic Office," Michael Allenson, The Protiviti View, 27 October 2001: https://blog.protiviti.com/2021/10/27/performance-over-presence-rethinking-the-post-pandemic-office/.

In their own role or in partnership with chief audit executives (CAEs), IT audit leaders should foster regular communications with senior management and the audit committee to keep both groups informed of the talent, skills and tools they need to sufficiently assess and monitor technology risk. IT audit leaders can also learn from CAEs and other functional leaders about the shortcomings of a workforce that relies too heavily on hiring and training and too little on a broader range of approaches to access needed talent, skills and tools. Recent Protiviti research on leading internal audit practices finds that an overreliance on training and developing staff to support innovation and transformation efforts could be placing inordinate demands on current staff and teams already stretched to capacity over the past several years.[7]

A growing number of organisational functions are accessing and embracing a diverse talent pool of full-time employees, contract and temporary workers, expert external consultants, and managed services and outsourcing providers. IT audit leaders and CAEs have an opportunity to recalibrate their labour models to ensure the entire future organisation can skill and scale to operate at the right size and in the right manner in the face of long-term talent crunches.[8]

Finally, there are concerns about the impact of these new working models (remote, hybrid, etc.) on the severity of technology risk to the enterprise. Close to half of IT audit leaders and professionals (45%) believe there will be a moderate impact on technology risk as a result of these changes in work models. The short- and long-term effects of these changes on the organisation's technology risk environment certainly bears monitoring by IT audit functions.

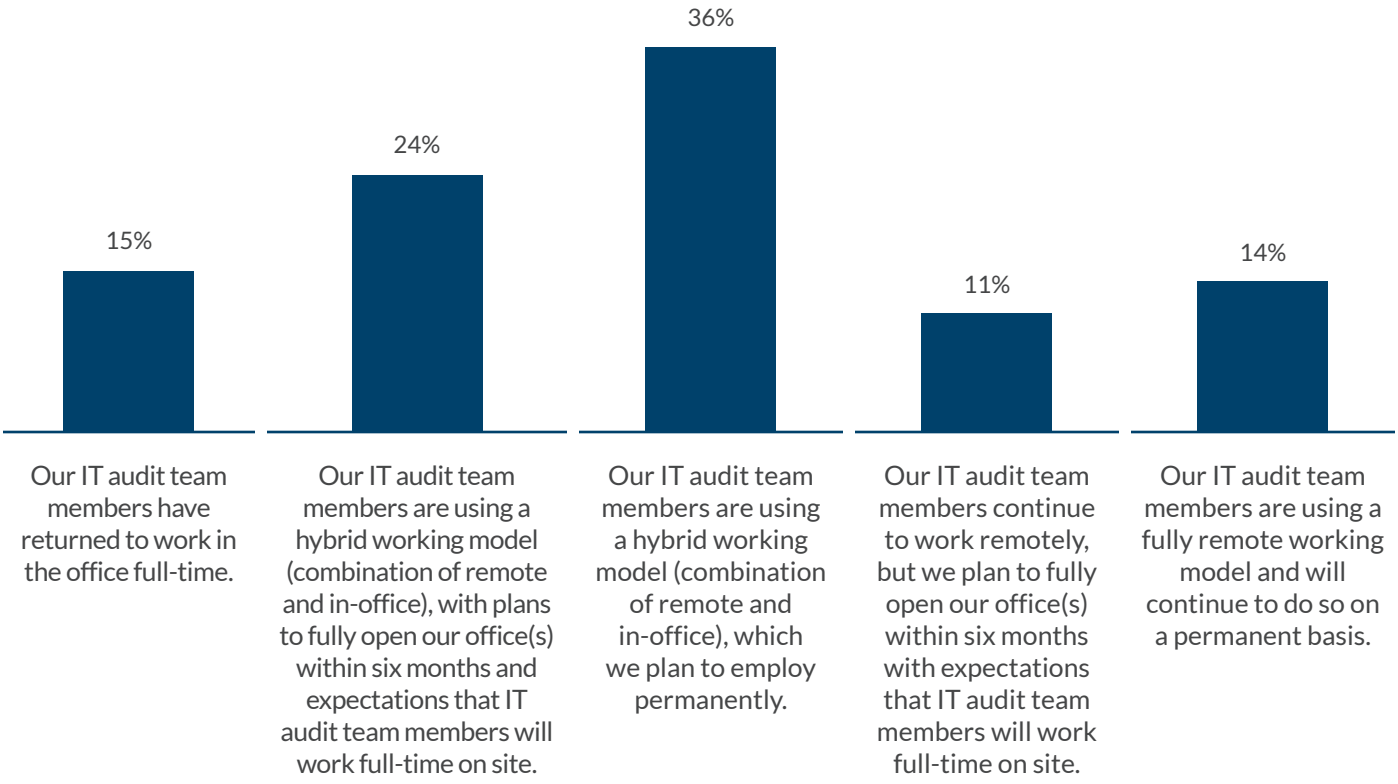
What percentage of your IT audit team do you think will work remotely full-time on a permanent basis moving forward?



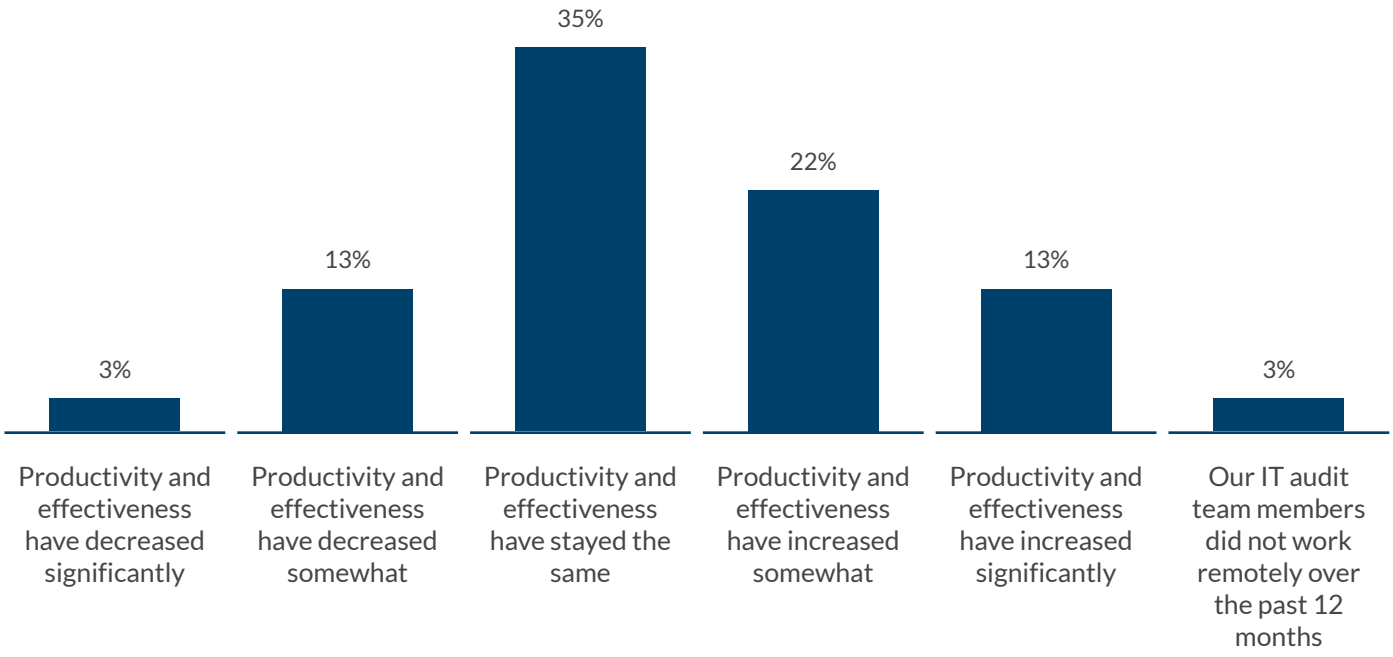
[7] *Innovation and Transformation Are Driving the Future of Internal Auditing*, Protiviti, March 2022: www.protiviti.com/US-en/insights/whitepaper-next-gen-internal-audit-survey.

[8] *Security, Data, Analytics, Automation, Flexible Work Models and ESG Define Finance Priorities*, Protiviti, September 2021: www.protiviti.com/US-en/insights/finance-trends-survey.

• • • Which of the following statements best describes the status of your IT audit team's working model?

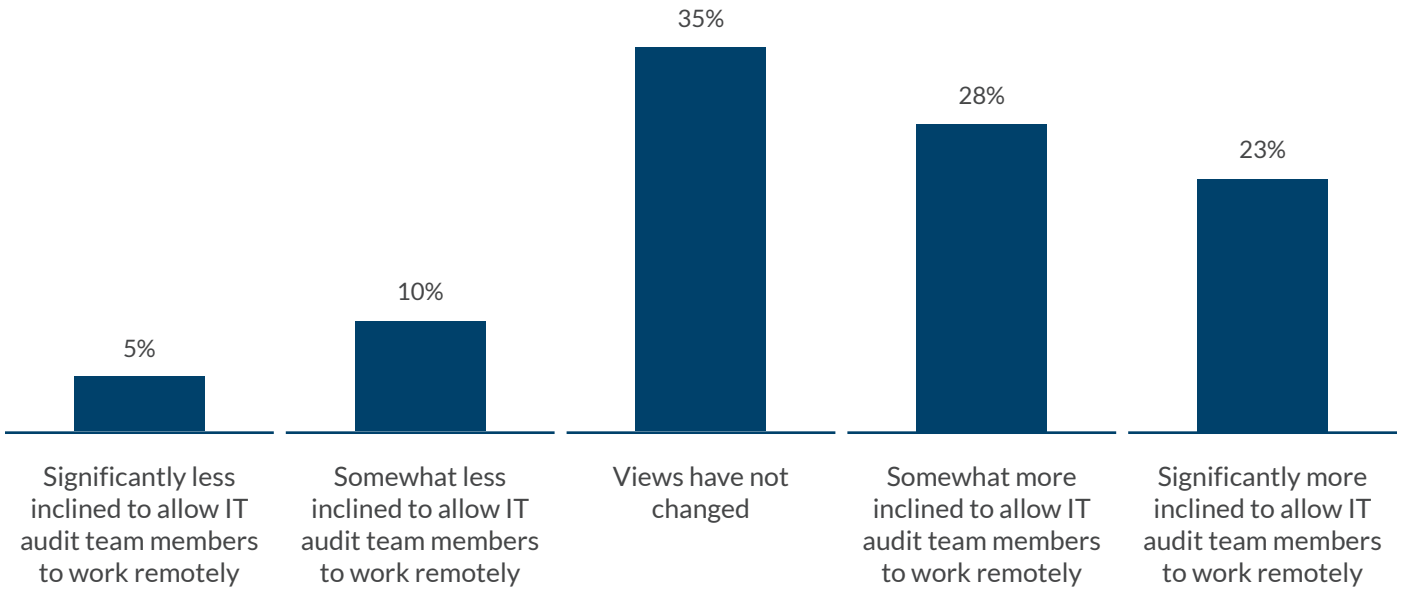


• • • How would you rate the overall level of productivity and effectiveness of your organisation's IT audit team members over the past 12 months as they have worked remotely or in a hybrid model?*

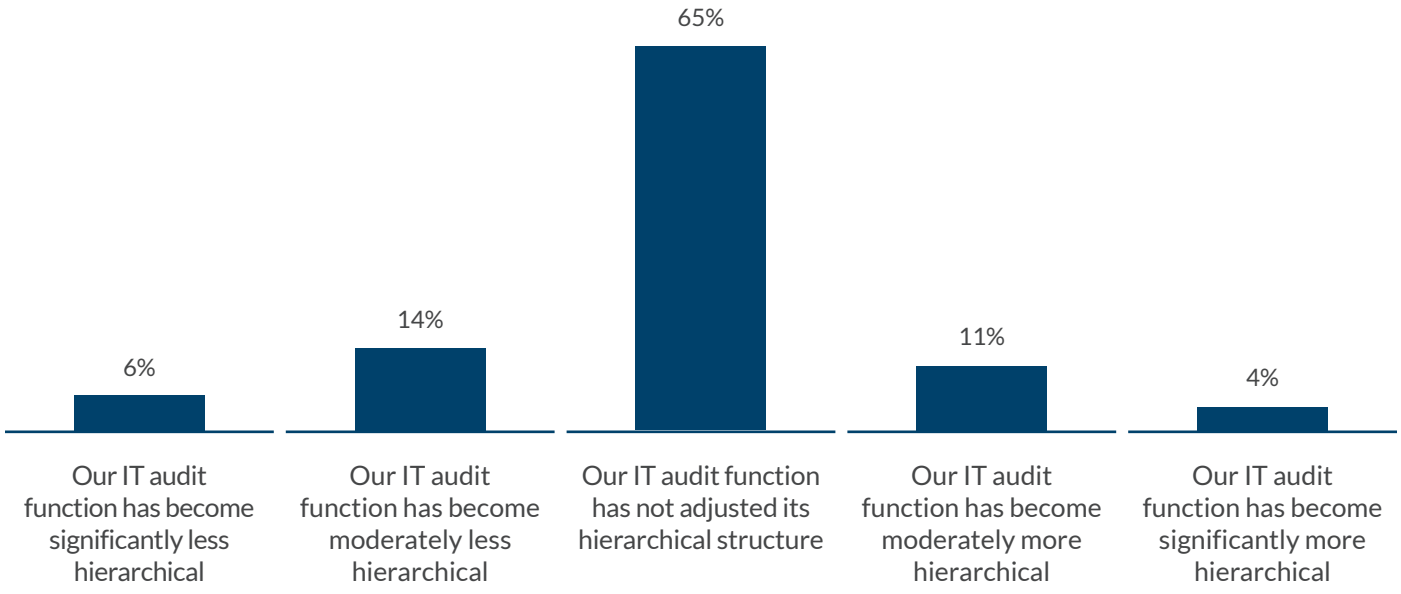


*Not shown: "Unsure" responses.

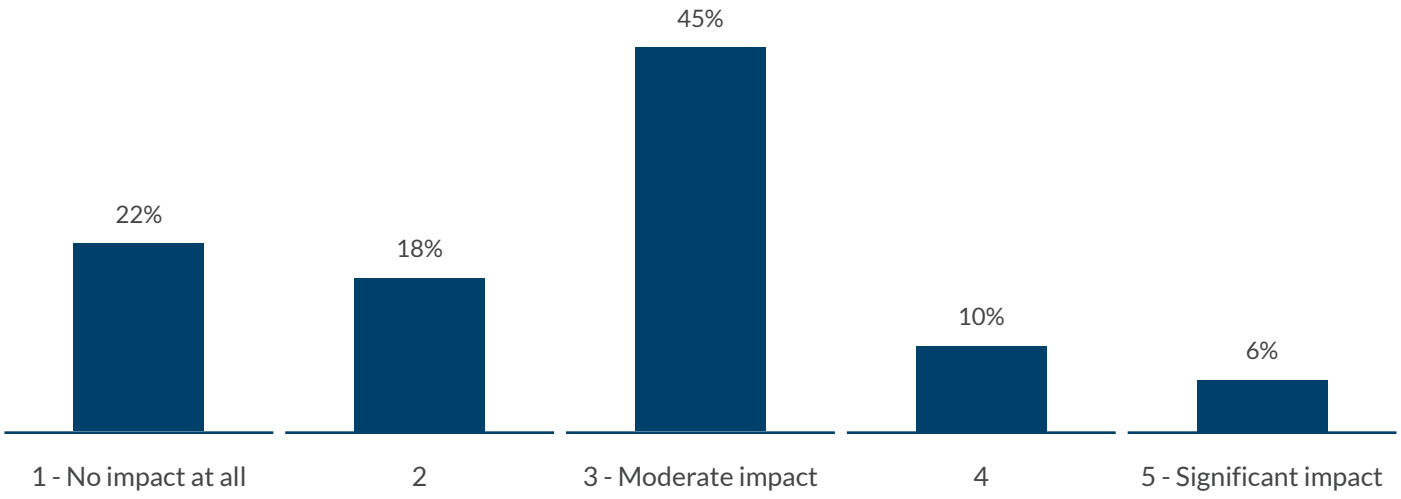
For the IT audit organisation in the post-pandemic world, how have your views changed with regard to IT audit leaders and staff members working remotely on a permanent basis?



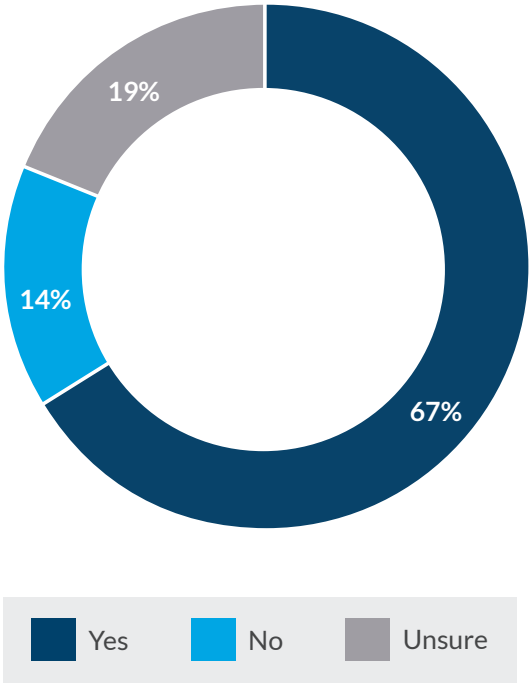
How, if at all, has your IT audit function adjusted its hierarchy in the past 12 months to address future needs?



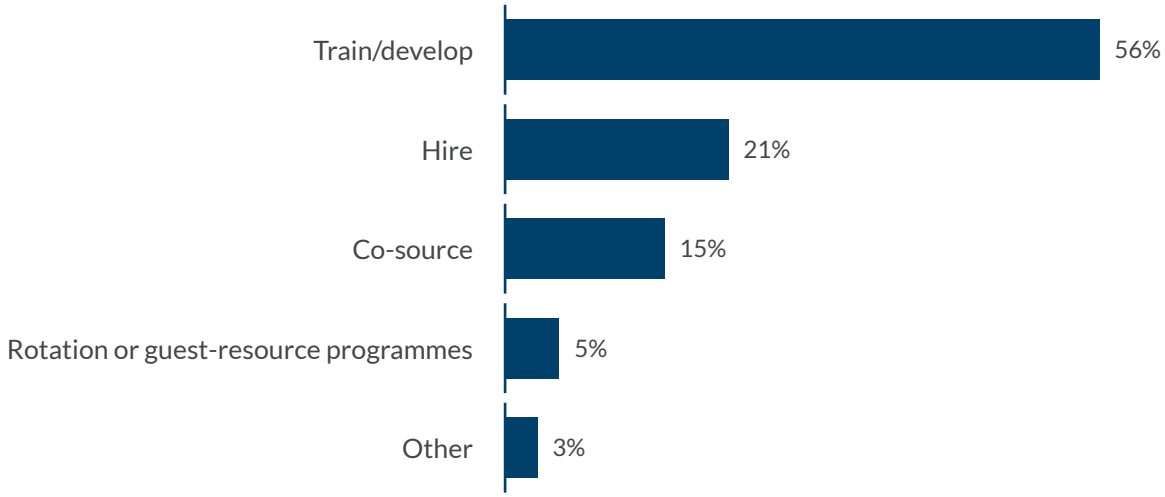
• • • How much, if at all, do you think the new model of work across your organisation (remote, hybrid, reduced work weeks, etc.) will impact the severity of technology risks to your organisation?



• • • Does your IT audit function have (or have access to) the necessary talent and skills?

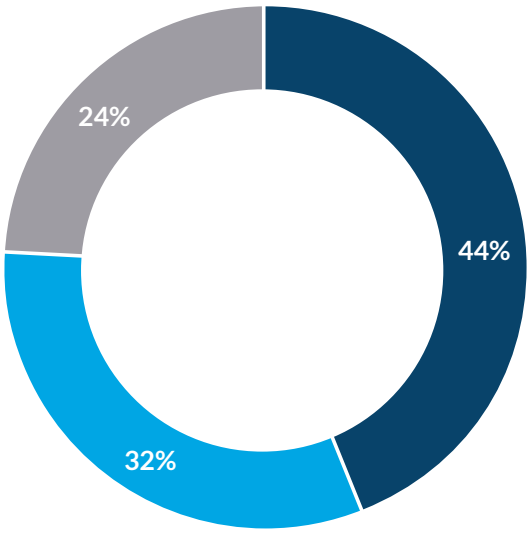


What is your primary strategy for the IT audit function?*



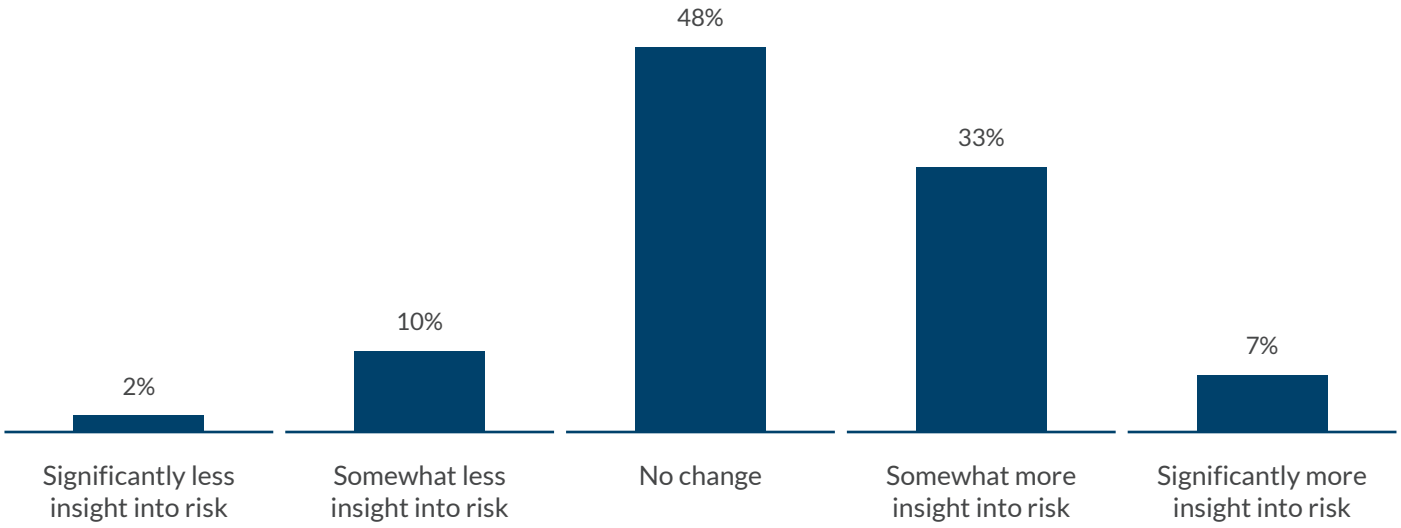
* Base: Organisations that have (or have access to) the necessary talent and skills

Do senior management and board/committees support acquiring or developing the necessary talent and skills?**



** Base: Organisations that do not have (or have access to) the necessary talent and skills

• • • How, if at all, has the IT audit team's level of insight into technology-related risks changed compared to pre-COVID levels?



In closing

Cybersecurity and breaches. Data governance and integrity. Regulatory compliance. Technology-enabled audits and risk assessments. Rethinking the office and talent strategy.

IT audit leaders unquestionably have a lot on their plate as they structure their functions and teams to address current and future demands along with technology risk issues their organisations must manage.

When it comes to these challenges, strategic-minded business leaders aren't thinking only about next quarter or next year; they're thinking about the next decade.[9] IT audit leaders across industries should embrace a similar mindset when addressing technology risk concerns as well as defining and executing the strategies and processes they use to assess and monitor them. The IT audit function of the future begins now.

[9] "It's the end of the work as we know it, and I feel fine," Joe Kornik, Vision by Protiviti, March 2022: https://vision.protiviti.com/insight/its-end-work-we-know-it-and-i-feel-fine.

Full list of technology risk issues, including definitions

Access risk — The organisation's access to information (data or programmes) or systems will be inappropriately granted or refused. This includes the risks of improper segregation of duties, risks associated with the integrity of data and databases, and risks associated with information confidentiality.

Access to talent and skills — The organisation lacks sufficient capacity and capability in IT resources or contractors to deliver upon the current and future technology needs of the organisation.

Change management — The organisation lacks clear and documented approaches to align, define, adopt and execute dynamic strategies for complex IT changes and transformation.

Cloud strategy and adoption — The organisation lacks a sufficiently robust cloud strategy and operating model that results in increased costs, system performance issues, and security or other controls compliance issues.

Cyber breach — The organisation is vulnerable to a cyber incident that could result in the compromise or disruption of data or systems that have a significant impact on business activities.

Data governance — The organisation lacks sufficient processes to ensure critical data assets are defined, and lacks a sufficient structure for cleansing, storing and reporting data in a way that makes it easy for the business to own and identify variances in its mission-critical information.

Data integrity — There is lack of clarity with regard to the authorisation, completeness and accuracy of transactions and other data as they are entered into, processed by, summarised by and reported on by the various application systems deployed by an organisation.

Develop and maintain application interfaces — Interfaces may not adopt a standardised approach ensuring completeness and integrity across the interface, with consistent error handling and alerting to related scheduling and incident management solutions to facilitate effective monitoring, reporting and intervention on a timely basis. New real-time message-based control architectures (e.g., confirmation mechanisms) may be required to provide completeness assurance.

Develop and maintain the IT governance structure — Different IT accountabilities, decision-making and oversight of IT activities are not well defined or understood by key stakeholders within IT and are not aligned to business governance, which could undermine decision-making and oversight.

Digital enablement — The company's existing operations, legacy IT infrastructure, and insufficient embrace of digital thinking and capabilities may not meet performance expectations related to quality, time to market, cost and innovation as well as competitive positioning, especially compared to those that are "born digital" and with a low-cost base for their operations, or compared to established competitors with superior operations.

Disaster recovery — The organisation lacks a comprehensive and documented disaster recovery plan for IT that could result in an extended disruption of IT services and performance.

Emerging technologies — The organisation's adoption of emerging technologies is not sufficiently governed, controlled or integrated with the broader IT strategy and results in operational disruptions to the business. Examples include: artificial intelligence, machine learning, robotic process automation, quantum computing, internet of things (IoT), augmented or virtual reality, and drone technology, among others.

Fit for purpose — Application systems have inadequate functionality, are not meeting business needs, and/or involve significant workarounds and/or manual intervention to enable business processes.

IT business enablement — The IT organisation is not adequately responsive to business needs, resulting in an impact to employee productivity, damage to company reputation or brand, missed technology-related innovation and opportunity identification, and higher operational costs.

IT capacity — The organisation has network/bandwidth limitations, insufficient storage or computing power, and/or an inability to scale other IT capabilities either internally or through service providers.

IT reliability and quality — The organisation does not properly maintain its technology infrastructure, leading to the loss of integrity, loss of availability, unacceptable latency, vendor support and end of life support/obsolescence.

Legacy infrastructure — The organisation lacks an effective information technology infrastructure (e.g., hardware, networks, software, people and processes) to effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion. In some instances, IT assets are obsolete, are no longer appropriately supported by the vendor and/or are past expected end of life.

Major projects — Major technology projects are significantly delayed and/or do not deliver the intended business outcomes.

Manage application change process — Application changes are adopting elements of an agile approach; however, inconsistent methods are being applied by different project teams, leading to user frustration and confusion over outcomes.

Manage employee training and awareness — The organisation lacks a process to conduct regular employee IT training, leading to underutilised systems and heightened security risk for the company.

Manage hardware maintenance agreements — The organisation has inadequate controls and monitoring of hardware maintenance arrangements, which could lead to increased risk of failures and resulting service outages. Unsupported hardware may not be identified for replacement when it is nearing end of support.

Manage security incidents — Security incidents are not identified, classified, routed and tracked to completion. Monitoring and escalation are not defined and/or effective to ensure incidents are appropriately prioritised and resolved on a timely basis to ensure meeting service requirements and to adequately respond and recover systems (where appropriate) from attacks and compromises (security).

Manage service losses or disruptions — The organisation is insufficiently prepared for an event that could lead to loss of, or disruption to, an organisation's operations, services or functions; there is not a clear process to identify, analyse and correct hazards to prevent a future re-occurrence.

Manage software licencing and compliance — Inadequate procurement, provisioning, tracking and monitoring controls over software can lead to non-compliance with licence obligations (and related penalties) or sub-optimal software licence costs being incurred. The use of products no longer supported may also give rise to security vulnerabilities where patching is no longer provided for such solutions.

Manage systems development life cycle (SDLC) — Developers may be adopting a range of new practices (e.g., Agile, DevOps) and models using third-party partners and code libraries without clear formal policies and an overall approach defined and communicated. This can lead to inconsistencies and/or a failure to adequately address control requirements (e.g., secure development, testing) during application development and technology adoption.

Manage technical infrastructure/services — There is not a clear overall process for operating, monitoring and maintaining the organisation's enterprise systems and resources to ensure that processing requirements for all business functions are met.

Manage IT assets — The organisation lacks sufficient processes to manage IT asset requests, procurement, accounting, deployment, monitoring and retirement.

Monitor regulatory compliance — Processes and controls are inadequate to identify new compliance requirements and changes to ensure they are addressed on a timely basis to meet compliance requirements. There is a lack of monitoring ongoing compliance and reporting.

Monitor/audit IT, legal and regulatory compliance — The organisation does not have a process to track the following related to technology: audit findings, remediation costs and fines, civil lawsuits, criminal charges, and regulators prevent doing business.

Operational processes lacking in intelligent automation — The organisation's IT operational processes are largely manual and thus error prone.

Operations — Inadequate disciplines and standardisation of operational processes are causing processing failures and business disruption.

Privacy — The organisation lacks sufficient controls and oversight of its data and compliance with privacy standards in jurisdictions in which it operates.

Project management risk — Especially with the adoption of agile change approaches, projects may not be managed consistently, leading to stakeholder confusion as to their oversight accountabilities, control points and standard artefact. This can undermine effective monitoring and successful delivery of anticipated benefits within planned timelines and resourcing.

Shadow IT/end user computing — The organisation lacks governance, oversight and control over decentrally utilised applications, systems and programmes, resulting in business-critical data potentially being at risk due to this data not being managed and protected to appropriate levels.

Strategy and alignment — The organisation's IT infrastructure, cloud environment and services lack sufficient alignment with the overall strategy of the business, including insufficient business enablement, poor planning and monitoring, or excessive operating costs.

Support the remote workplace infrastructure — The organisation lacks sufficient tools, technologies and resources to enable and support a remote workforce for an extended period.

Technology innovation — The organisation is not leveraging new technologies in its business model in comparison to competitors and new entrants.

Third-party risk — The organisation lacks sufficient skills, knowledge and ability to govern its third parties, including their agreements, overall operations and security, as well as the organisation's critical data and processes outsourced to third parties.

Methodology and demographics

ISACA and Protiviti partnered to conduct the 10th annual IT Audit Technology Risks Study in the fourth quarter of 2021. More than 7,500 (n = 7,591) executives and professionals, including CAEs as well as IT audit vice presidents and directors, completed our online questionnaire.

Since completion of the survey was voluntary, there is some potential for bias if those choosing to respond have significantly different views on matters covered by the survey from those who did not respond. Therefore, our study's results may be limited to the extent that such a possibility exists. In addition, some respondents answered certain questions while not answering others. There is also a disparity in the number of responses from each geographic region. Despite these inherent limitations, we believe the survey results provide valuable insights regarding IT audit practices in organisations today.

Position

Chief Audit Executive (or equivalent)	4%
IT Executive	4%
IT Risk/Control Executive	3%
IT Audit Director	4%
Audit Director	2%
IT Audit Manager	11%
Audit Manager	5%
IT Manager	11%
IT Risk/Control Manager	10%
IT Audit Staff	12%
Audit Staff	4%
IT Risk/Control Specialist	11%
Other	19%

Industry

Financial Services — Banking	18%
Government	11%
Technology (Software/High-Tech/Electronics)	10%
Tech Services Consulting	7%
Professional Services	7%
Insurance (other than Healthcare Payer)	5%
Financial Services — Other	4%
Telecommunications and Data Infrastructure	4%
Healthcare Provider	3%
Manufacturing (other than Technology)	3%
Retail	2%
Financial Services — Asset Management	2%
Higher Education	2%
Power and Utilities	2%
Oil and Gas	1%
Transportation and Logistics	1%
Financial Services — Payments	1%
Automotive	1%
Financial Services — Broker-Dealer	1%
Not-for-profit	1%
Healthcare Payer	1%
Pharmaceuticals and Life Sciences	1%
Hospitality, Leisure and Travel	1%
Consumer Packaged Goods	1%
Real Estate	1%
Wholesale and Distribution	1%
Media	1%
Agriculture, Forestry and Fishing	1%
Construction	1%
Other	5%

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

$20 billion or more	18%
$10 billion - $19.99 billion	6%
$5 billion - $9.99 billion	7%
$1 billion - $4.99 billion	16%
$500 million - $999.99 million	10%
$100 million - $499.99 million	14%
Less than $100 million	29%

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

$250 billion or more	26%
$50 billion - $249.99 billion	10%
$25 billion - $49.99 billion	6%
$10 billion - $24.99 billion	11%
$5 billion - $9.99 billion	9%
$1 billion - $4.99 billion	14%
Less than $1 billion	24%

Organisational type

Publicly traded	35%
Private	43%
Government	14%
Not-for-profit	5%
Other	3%

Organisational headquarters

United States	48%
United Kingdom	5%
Japan	4%
India	4%
Australia	2%
Canada	2%
Hong Kong	2%
The Netherlands	2%
Germany	2%
Singapore	2%
Switzerland	2%
China	1%
France	1%
South Africa	1%
United Arab Emirates	1%
Spain	1%
Nigeria	1%
South Korea	1%
Kenya	1%
Philippines	1%
Saudi Arabia	1%
Italy	1%
Ireland	1%
Malaysia	1%
Other	12%

IT audit department headquarters

United States	47%
India	5%
Japan	4%
United Kingdom	3%
Australia	3%
Canada	2%
Hong Kong	2%
Singapore	2%
Germany	2%
The Netherlands	2%
China	1%
Switzerland	1%
South Africa	1%
United Arab Emirates	1%
Spain	1%
Nigeria	1%
South Korea	1%
France	1%
Philippines	1%
Kenya	1%
Italy	1%
Saudi Arabia	1%
Malaysia	1%
Mexico	1%
Turkey	1%
Other	13%

Audit department headcount

0-4	18%
5-9	13%
10-19	14%
20-29	8%
30+	47%

Total number of full-time IT auditors

0	7%
1	13%
2	10%
3	8%
4	5%
5	8%
6-10	14%
11+	35%

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, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2022 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.

ABOUT ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its more than 165,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

Participate in the ISACA Knowledge Center: www.isaca.org/resources

Follow ISACA on Twitter: www.twitter.com/ISACANews

Join ISACA on LinkedIn: ISACA (Official), www.linkedin.com/company/ISACA

Like ISACA on Facebook: www.facebook.com/ISACAHQ

isaca.org

protiviti®

protiviti.com