ISACA

protiviti®
Face the Future with Confidence

IT Audit's Perspectives on the Top Technology Risks for 2021

Cybersecurity, privacy, data and resilience dominate the top technology challenges for organisations, according to the annual ISACA/Protiviti global survey of IT audit leaders and professionals

The most significant technology risks for 2021 reflect our COVID-19 world and its impact on business conditions and priorities. What's increasingly apparent is that more digitally mature organisations have a clear advantage.

In September/October 2020, ISACA and Protiviti conducted a global survey of more than 7,400 IT audit and risk leaders and professionals to obtain their perspectives on the top technology risks their organisations will face in 2021. We also addressed the impact of the COVID-19 global pandemic as well as ongoing digital transformation efforts.

The results are enlightening, with cybersecurity and privacy issues, regulatory compliance, data, disaster recovery, and other pandemic-driven concerns ranking among the top technology risks for organisations globally. Interestingly, the top technology risk issues are generally consistent across different industries and regions, yet there are noticeable differences between organisations we classify as Digital Leaders and other organisations (we define our Digital Leader categorisation on pages 7-8). The risks, which reflect our current times, provide a clear roadmap for IT audit functions as to where they should focus their attention and energy in 2021.

From their commitment to continual risk assessments to their perception of virtually all technology risk issues to be more significant compared to other organisations, Digital Leaders are able to see their organisation in different ways, which is to their advantage.

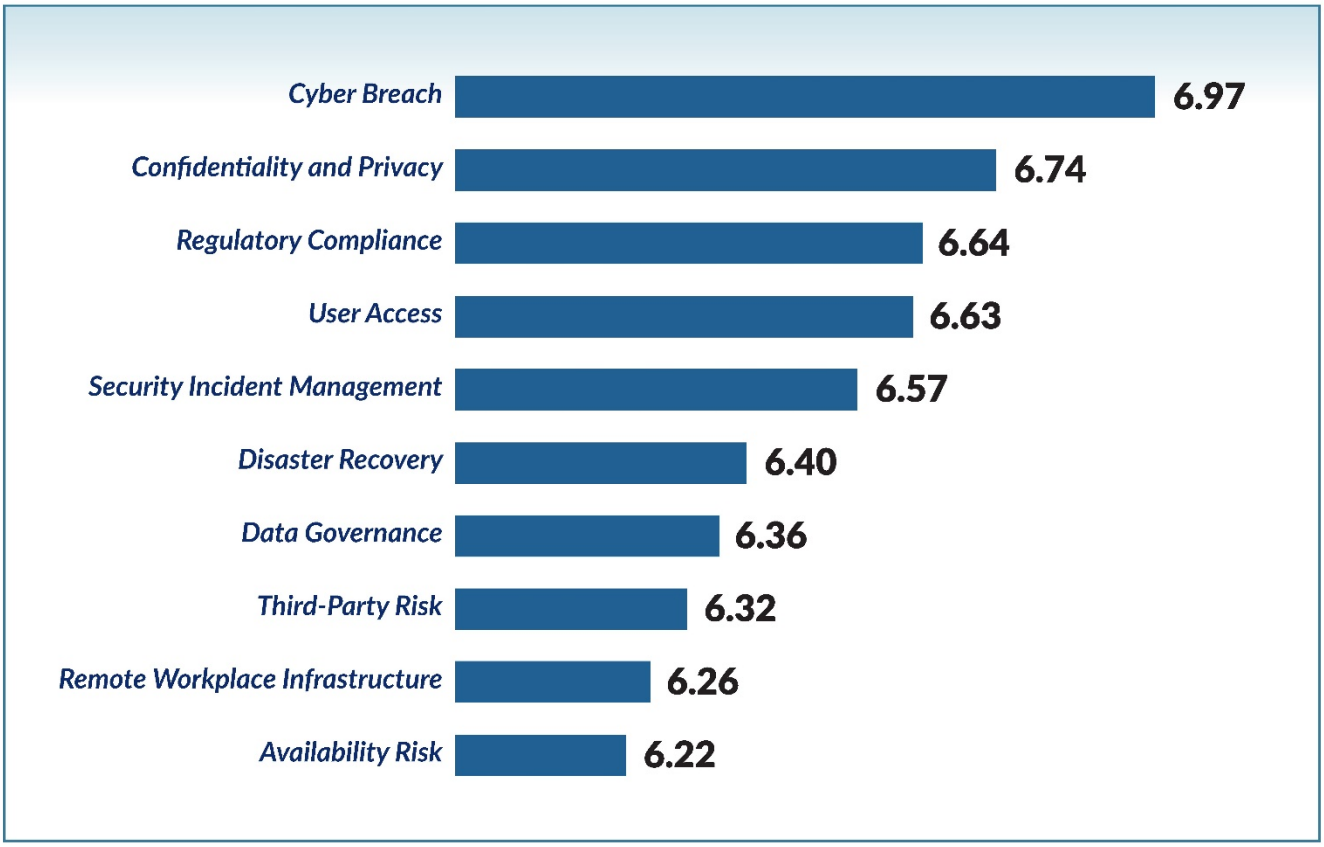
Our notable findings:

Security, privacy and resilient technologies dominate the top technology risks – These issues, which already were top-of-mind risks for most organisations, have been heightened by pandemic-driven times of remote work and new business processes, as well as increasing connectivity via the Internet of Things (IoT). The highest-rated risks also represent higher-velocity issues for organisations.

Digital Leaders stand out – Organisations at a higher level of digital maturity, understanding the need for dynamism in the current business environment, generally view the top technology risks to be more significant compared to other organisations, and they are far more likely to perform continuous audit risk assessments.

COVID-19 and digital transformation are driving more frequent technology risk assessments – As expected, IT audit groups are refreshing technology risk assessments more frequently in response to pandemic-related impacts and digital transformation-driven changes in the organisation.

Global Top 10 Technology Risks for 2021*



** About our top technology risks scale*: Respondents were asked to rate the significance of 39 technology risk issues on a scale of 1 to 10, based on their organisation's technology risk assessment, with "1" representing low impact to the organisation and "10" representing extensive impact to the organisation. Data points represent the mean score.

About Our Survey – Taking a New Approach

After many years conducting a well-received global study in which we benchmarked numerous aspects of IT audit functions, ISACA and Protiviti decided to adopt a new approach. Rather than address the broad spectrum of IT audit group operations, we decided to focus more specifically on the views of IT audit leaders and professionals about the technology risk issues their organisations are facing over the next 12 months. This element of our prior study had proven increasingly popular with our readers and we recognised an opportunity to build on this by presenting a framework in which technology risks could be rated on a 1-10 scale based on level of significance to an organisation.[1] In addition, we wanted to assess more closely the advantages of digitally mature organisations in addressing technology risks.

We also included brief sections addressing the impact of the COVID-19 global pandemic and broader digital transformation efforts, as well as the technology risk assessment process.

For further information about our survey, please see the Methodology and Demographics section.

[1] ISACA's Risk IT Framework is designed to assist in developing, implementing, or enhancing the practice of risk management by:
- Connecting the business context with the specific information and technology assets
- Shifting the focus to activities over which the enterprise has significant control, such as actively directing and managing risk, while minimising the focus on the conditions over which an enterprise has little control (threat actors)
- Increasing the focus on using a common risk language that correctly labels the items that have to be managed well to create value

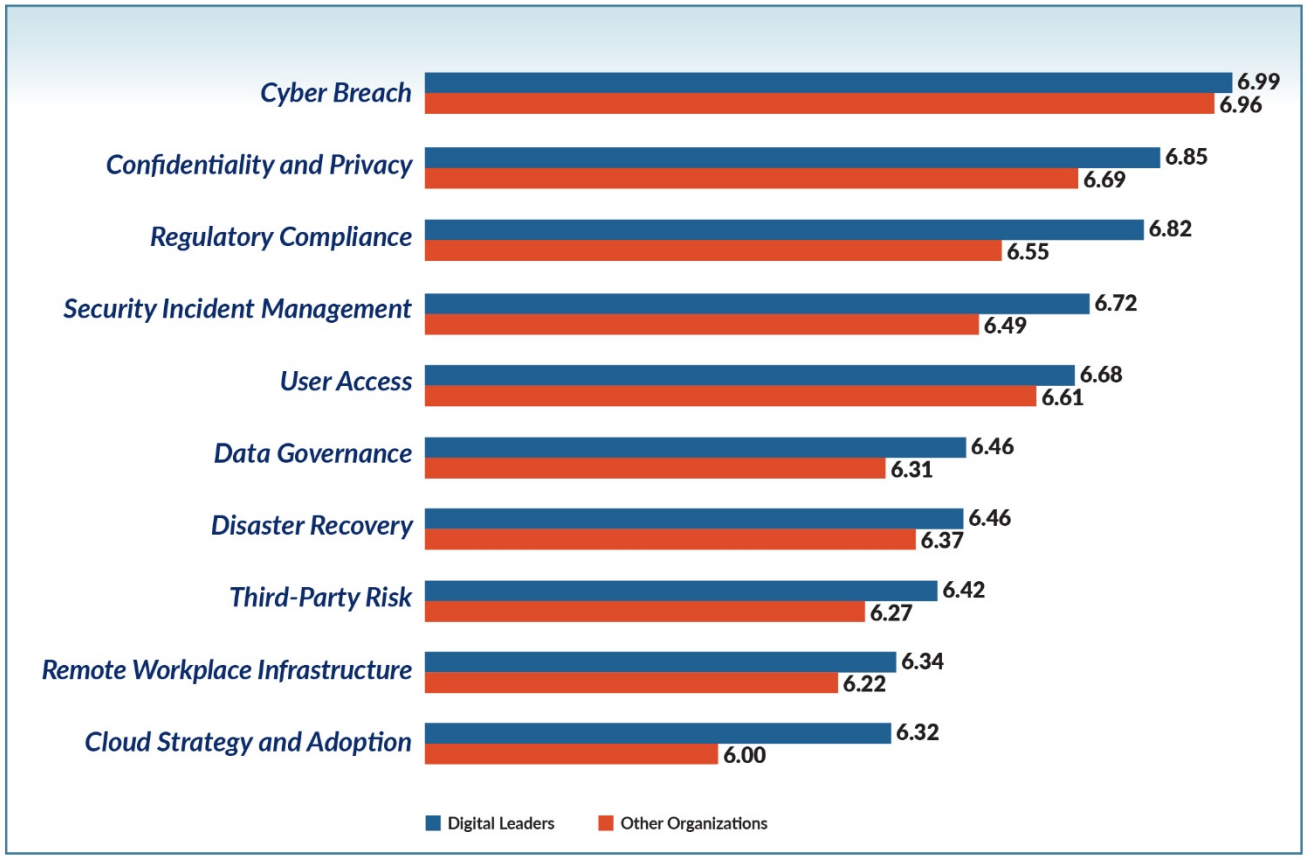
The framework will enable enterprises to understand and manage all significant IT risk types, building upon the existing risk-related components within the current ISACA frameworks. For more information, visit www.isaca.org/bookstore/bookstore-risk-digital/ritf2.

How Digital Leaders Differentiate Themselves

What You Need to Know

- The top 10 technology risks for Digital Leaders are relatively consistent with other organisations, though most of the data points trend higher for Digital Leaders. This is telling – given the greater frequency of their technology risk assessment process, Digital Leaders may have a clearer view of the specific risks affecting their organisations.
- There is one notable difference: "Cloud strategy and adoption" is a top 10 technology risk issue for Digital Leaders but not other organisations, given what is a heightened focus among Digital Leaders to include cloud technologies in their delivery of business services, as well as in their longer-term planning and strategy.

Global Top 10 Technology Risks – Digital Leader Group vs. Other Organisations



Commentary

Digital Leaders have incorporated more advanced technologies (such as intelligent automation, IoT, artificial intelligence and machine learning) into their organisations and processes, and they generally make more extensive use of data and technology to support enhanced customer engagement and operational performance as well as the digitisation of products and services. Greater, and more integrated, use of data and technology as well as generally more complex technology environments understandably elevate perceived risk levels with regard to security, privacy and data.

On the other hand, organisations outside the Digital Leader group may have less visibility into what they do not know. In general, these organisations operate in less agile ways and with lower levels of data and technology enablement.

The top-rated technology risk issues clearly indicate concerns around security, privacy, cloud and technology resilience that were further fuelled by shifting business priorities, the pandemic-induced remote work environment, and the accelerated deployment of new technologies. Our survey results suggest the most highly rated issues for 2021 tend to be high-velocity risks (e.g., cyber breach, privacy, user access, disaster recovery), while longer-term foundational risks are slower moving and appear in the bottom half of the overall technology risk rankings for the coming year (e.g., talent and skills, legacy infrastructure, IT business enablement, IT governance). While this is understandable in today's dynamic and unpredictable climate, it's also important for organisations not to defer handling risks that are slower-moving but still have the potential for major impact over time.

About Our Digital Maturity Scale

In our study, respondents were asked to rate the digital maturity of their organisation on a 10-point scale (see below). The question included a detailed definition of digital transformation and maturity:

> *Digital transformation is about changing the way an organisation acts and thinks in everything it does to position it to compete with "born digital" companies and Digital Leaders, including through increased use of data and technology to support enhanced customer engagement, digitisation of products and services, better informed decision making, and improved operational performance. We define the levels of digital maturity as follows:*

- **Digital Skeptic**: Digital plans are not formalised and initiatives are managed in an ad hoc or reactive manner. React to competition. Risk averse.
- **Digital Beginner**: Digital plans are not fully developed, although multiple digital initiatives are underway and the objectives of these initiatives are understood. Embracing change. Collection of point solutions.
- **Digital Follower**: A digital strategy has been developed and the organisation has a proven track record of delivering on digital initiatives. Digital initiatives are typically focused on discrete aspects of the customer journey. Clear strategy. Agile. Effective at change delivery.
- **Digital Expert**: Digital aspects are in place and managed quantitatively enterprisewide. High levels of process automation have been achieved. The organisation has a proven track record adopting emerging technologies. Low cost base. Hyper scalable.
- **Digital Leader**: The organisation has a proven track record of disrupting traditional business models. Digital aspects of strategic plans are continually improved based on lessons learned and predictive indicators. Innovative. Disruptive.

Digital Maturity Scale

1 – Digital Sceptic

2 – Digital Sceptic +

3 – Digital Beginner

4 – Digital Beginner +

5 – Digital Follower

6 – Digital Follower +

7 – Digital Expert -

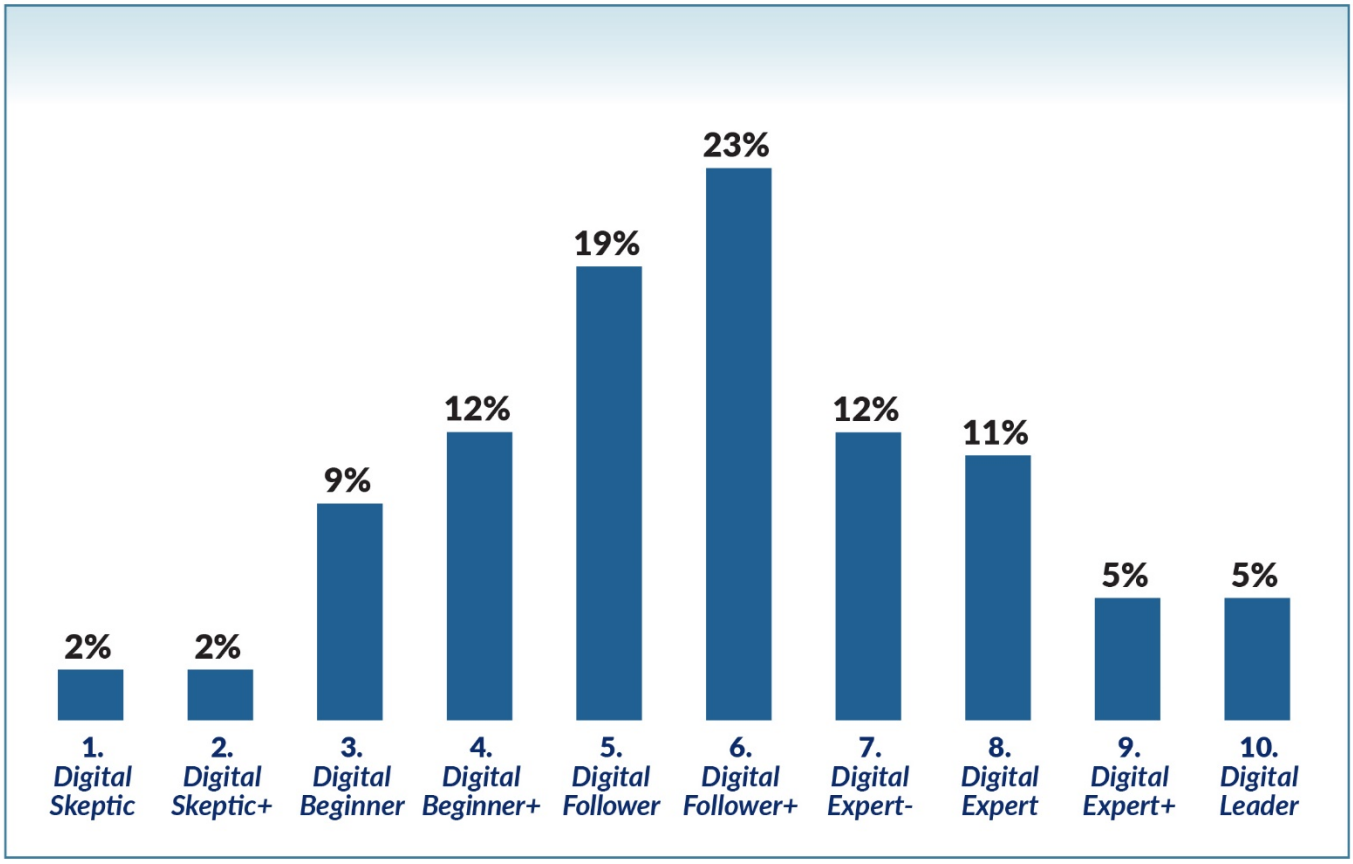
8 – Digital Expert

9 – Digital Expert +

10 – Digital Leader

For the purpose of our analysis, we have categorised our group of "Digital Leaders" to include those organisations that rank themselves at "7" or higher.

Where Organisations Rank on the Digital Maturity Scale



Impact of COVID-19 and Digital Transformation – Frequency of Technology Risk Assessments Is Rising

What You Need to Know

- Most organisations are identifying and assessing technology risk for the purposes of audit planning – a positive development.
- Compared to other organisations, Digital Leaders stand out in their frequency of performing technology audit risk assessments, driven by more agile ways of working, as well as more integration and use of data and technology. Close to a majority of Digital Leaders identify and assess technology risk continually – i.e., more frequently than on a monthly basis.
- Of note, 11% of organisations that are not classified as Digital Leaders are not conducting any form of technology risk assessment.

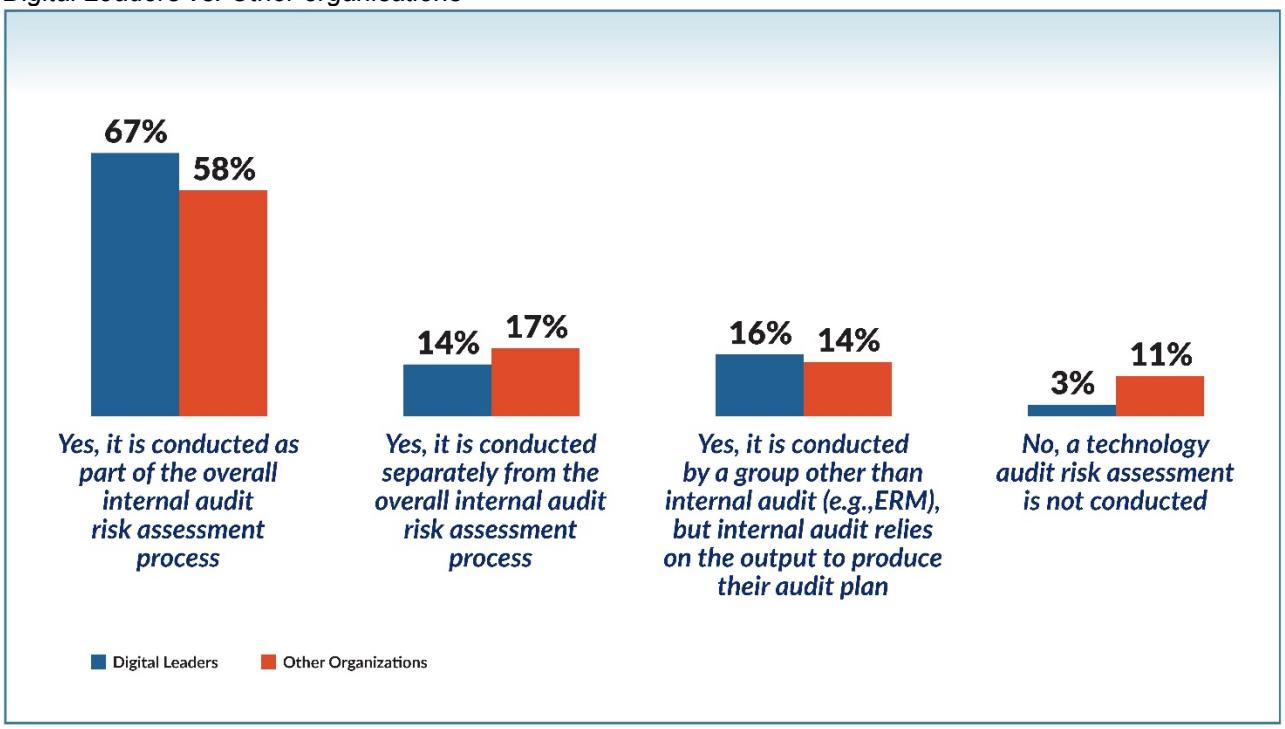
Does your organisation identify and assess technology risk for audit planning purposes?

	All respondents
Yes, it is conducted as part of the overall internal audit risk assessment process	61%
Yes, it is conducted separately from the overall internal audit risk assessment process	16%
Yes, it is conducted by a group other than internal audit (e.g., ERM), but internal audit relies on the output to produce their audit plan	15%
No, a technology audit risk assessment is not conducted	8%

Note: The "Yes" responses to this question represent the respondent base for a number of other questions and results in our study, as reported in this paper.

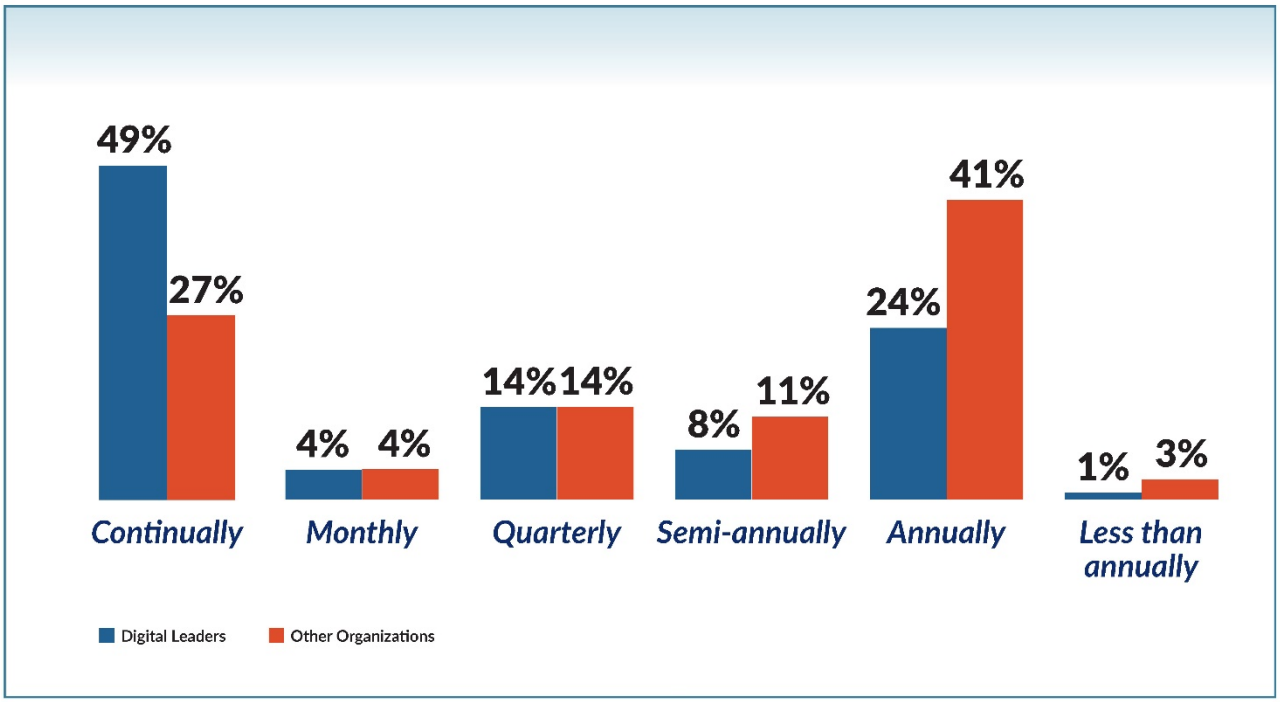
Does your organisation identify and assess technology risk for audit planning purposes?

Digital Leaders vs. Other organisations



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

Digital Leaders vs. Other organisations



* Base: Respondents whose organisations identify and assess technology risk for audit planning purposes.

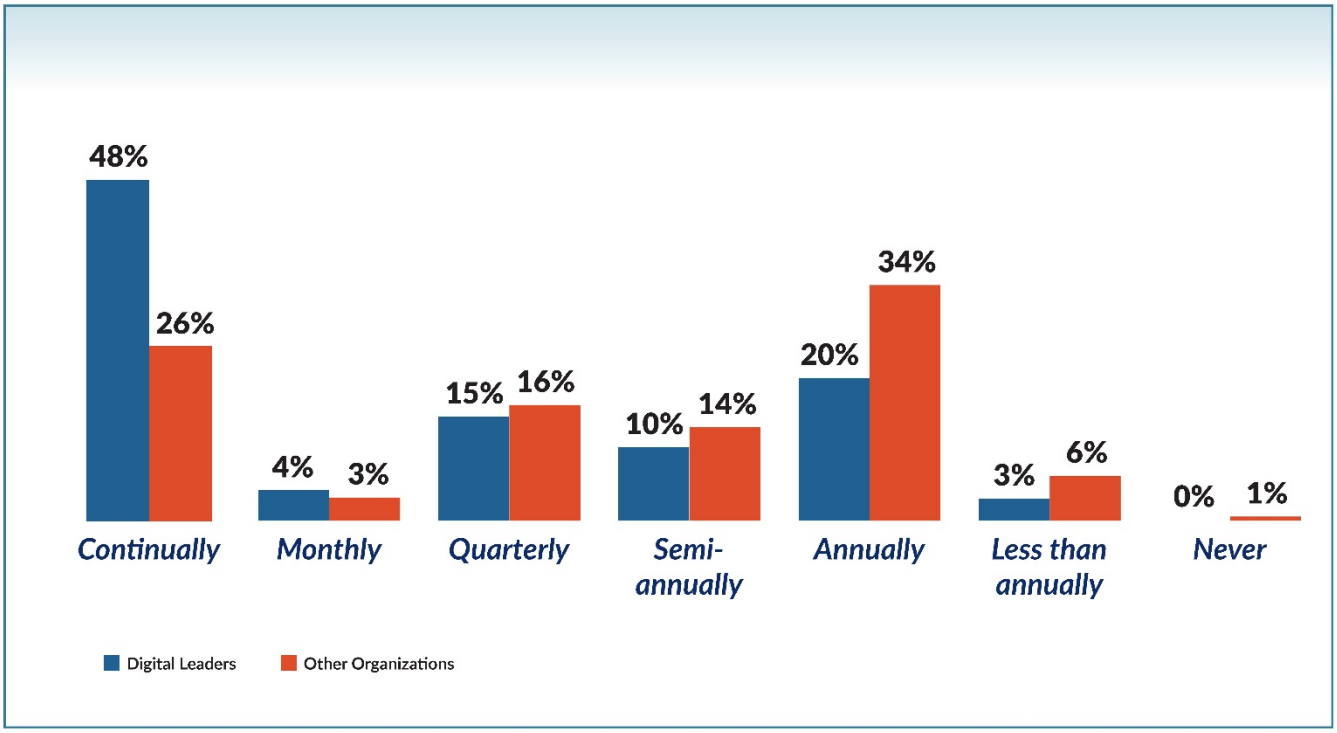
Will digital transformation efforts impact the frequency of updates made to your organisation's technology audit risk assessment? (Shown: "Yes" responses)*

Digital Leaders

Other organisations

How frequently will your technology audit risk assessment be updated due to digital transformation changes within your organisation?*

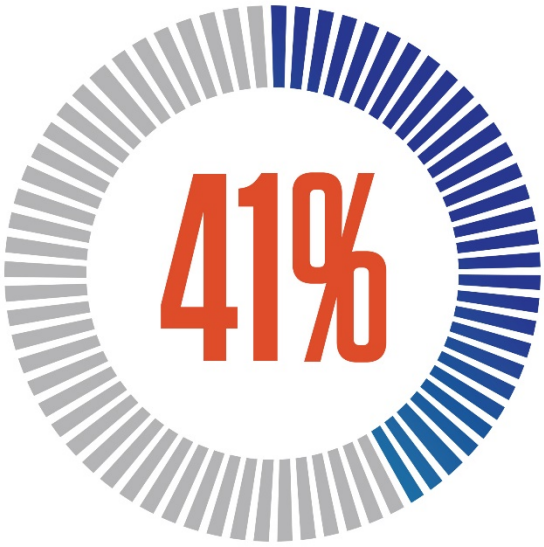
Digital Leaders vs. Other organisations



* Base: Respondents whose organisations identify and assess technology risk for audit planning purposes.

Have COVID-related disruptions and related changes to business conditions caused you to adjust the nature or frequency of technology risk assessments?* (Shown: "Yes" responses)

Digital Leaders



Other organisations

*Base: Respondents whose organisations identify and assess technology risk for audit planning purposes.

Commentary

As more Digital Leaders understand, identifying and assessing technology risks on a more dynamic and frequent basis facilitates the development of closer-to-real-time views of risk and allows them to be more agile and responsive to the rapidly evolving risk landscape. These are the hallmarks of dynamic risk assessment.

Amid an organisation's digital transformation journey, continuous risk assessments and more risk-responsive and risk-aligned audits are essential to delivering feedback and value early and often to stakeholders and the business. This is particularly important as the business environment continues to experience rapid change due to the COVID-19 global pandemic, digital transformation and other disruptive forces. A dynamic risk assessment approach enables IT audit groups to be increasingly precise in assessing and adapting to emerging risks. This capability, in turn, helps organisations identify changing risk trends closer to real time, more data-driven ways to measure and prioritise risk, and ultimately more efficient and effective risk assurance.

Of note, certain organisations (3% of Digital Leaders and 11% of other organisations) report that they do not conduct a technology audit risk assessment. While a bit surprising, it is possible that within some of these organisations, IT risk assessment is more tightly integrated into the overall risk assessment process.

Industry Frameworks

What You Need to Know

- COBIT is the most frequently used framework to identify and assess technology risk in organisations. Digital Leaders rely on this framework at a slightly higher level than other organisations. In addition, while close to a majority of smaller organisations use this framework, COBIT is used substantially more by larger organisations.
- The ISO 27000 Series and NIST Cybersecurity Framework are used by close to a majority of all organisations, with Digital Leaders relying on these two frameworks significantly more than other organisations.

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

	All respondents
COBIT	58%
ISO 27000 Series	49%
NIST Cybersecurity Framework	48%
COSO Internal Controls – Integrated Framework	39%
ITIL	35%
Government-issued guideline	31%
Industry initiative guideline	19%
CIS Critical Security Controls	15%
FFIEC Cybersecurity Assessment Tool	11%
CSA Cloud Controls Matrix	10%
FAIR Cyber Risk Framework	4%
Other	4%

* Base: Respondents whose organisations identify and assess technology risk for audit planning purposes.

Framework Definitions

- **COBIT**: Created by ISACA for information technology management and IT governance.
- **ITIL**: A set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.
- **COSO Internal Controls – Integrated Framework**: Provides principles-based guidance for designing and implementing effective internal controls.
- **FFIEC Cybersecurity Assessment Tool**: Helps financial institutions identify their risks and determine their cybersecurity preparedness.
- **NIST Cybersecurity Framework**: Helps organisations to better understand and improve their management of cybersecurity risk.
- **ISO 27000 Series**: Information security standards published jointly by the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC).
- **CIS Critical Security Controls**: Prioritised set of actions to protect the organisation and data from known cyber attack vectors.
- **CSA Cloud Controls Matrix**: Cybersecurity control framework for cloud computing.
- **FAIR Cyber Risk Framework**: Provides information risk, cybersecurity and business executives with standards and best practices to measure, manage and report on information risk from the business perspective.

Appendix

Top 10 Technology Risks by Industry Group

More detailed industry results are available upon request.

Consumer Packaged Goods/Retail

	Average Score
Confidentiality and Privacy	6.97
Cyber Breach	6.89
User Access	6.86
Data Governance	6.62
Cloud Strategy and Adoption	6.53
Major Projects	6.51
Third-Party Risk	6.37
Remote Workplace Infrastructure	6.37
Disaster Recovery	6.36
Security Incident Management	6.33

Energy and Utilities

	Average Score
Cyber Breach	7.14
Regulatory Compliance	6.59
User Access	6.58
Security Incident Management	6.56
Disaster Recovery	6.53
Third-Party Risk	6.51
Confidentiality and Privacy	6.44
Data Governance	6.44
Availability Risk	6.37
Service Losses or Disruptions	6.29

Financial Services

	Average Score
Cyber Breach	7.27
Regulatory Compliance	7.17
Confidentiality and Privacy	7.03
User Access	6.94
Security Incident Management	6.90
Third-Party Risk	6.77
Disaster Recovery	6.73
Data Governance	6.69
Remote Workplace Infrastructure	6.57
Availability Risk	6.54

Healthcare

	Average Score
Cyber Breach	7.24
Confidentiality and Privacy	6.92
User Access	6.89
Regulatory Compliance	6.88
Security Incident Management	6.64
Third-Party Risk	6.64
Availability Risk	6.52
Disaster Recovery	6.44
Service Losses or Disruptions	6.20
Data Governance	6.16

Manufacturing and Distribution

	Average Score
Cyber Breach	6.88
User Access	6.65
Confidentiality and Privacy	6.50
Security Incident Management	6.30
Regulatory Compliance	6.27
Disaster Recovery	6.26
Third-Party Risk	6.26
Data Governance	6.20
Major Projects	6.06
Service Losses or Disruptions	6.05

Technology, Media and Telecommunications

	Average Score
Cyber Breach	6.92
Confidentiality and Privacy	6.63
Security Incident Management	6.59
Regulatory Compliance	6.53
User Access	6.53
Disaster Recovery	6.39
Data Governance	6.33
Service Losses or Disruptions	6.31
Cloud Strategy and Adoption	6.23
Availability Risk	6.23

Top 10 Technology Risks by Region

More detailed regional results are available upon request.

Africa

	Average Score
Cyber Breach	6.61
Confidentiality and Privacy	6.35
Disaster Recovery	6.30
Security Incident Management	6.19
Data Governance	6.14
Major Projects	6.12
Remote Workplace Infrastructure	6.09
Service Losses or Disruptions	6.07
User Access	6.02
Regulatory Compliance	5.97

Asia

	Average Score
Cyber Breach	6.48
Confidentiality and Privacy	6.46
Security Incident Management	6.32
Remote Workplace Infrastructure	6.23
Regulatory Compliance	6.22
User Access	6.20
Disaster Recovery	6.15
Data Governance	6.10
Availability Risk	5.95
Service Losses or Disruptions	5.95

Europe

	Average Score
Cyber Breach	7.18
Confidentiality and Privacy	6.98
Regulatory Compliance	6.90
User Access	6.84
Security Incident Management	6.74
Disaster Recovery	6.55
Data Governance	6.54
Availability Risk	6.46
Third-Party Risk	6.44
Service Losses or Disruptions	6.36

Latin America

	Average Score
Confidentiality and Privacy	7.29
Disaster Recovery	7.23
Cyber Breach	7.21
Security Incident Management	7.10
User Access	7.08
Regulatory Compliance	6.92
Monitor/Audit IT, Legal and Regulatory Compliance	6.74
Availability Risk	6.66
Service Losses or Disruptions	6.66
Integrity	6.60

Middle East

	Average Score
Cyber Breach	6.99
Disaster Recovery	6.85
User Access	6.84
Security Incident Management	6.80
Confidentiality and Privacy	6.79
Regulatory Compliance	6.62
Availability Risk	6.51
Data Governance	6.47
Integrity	6.39
Service Losses or Disruptions	6.32

North America

	Average Score
Cyber Breach	7.04
Confidentiality and Privacy	6.72
Regulatory Compliance	6.72
User Access	6.71
Security Incident Management	6.56
Third-Party Risk	6.46
Data Governance	6.36
Disaster Recovery	6.32
Cloud Strategy and Adoption	6.28
Remote Workplace Infrastructure	6.22

Oceania

	Average Score
Cyber Breach	7.67
Confidentiality and Privacy	7.16
User Access	7.03
Regulatory Compliance	6.93
Major Projects	6.80
Disaster Recovery	6.79
Security Incident Management	6.78
Data Governance	6.76
Availability Risk	6.73
Third-Party Risk	6.62

Full list of technology risk issues, including definitions

Access to Talent and Skills – The organisation lacks sufficient capacity or capability in IT resources or contractors to deliver upon the current and future technology needs of the organisation.
Application Change Process – Change management processes are not sufficiently mature to ensure changes to IT systems do not cause operational disruption or a reduction in user experience, or introduce vulnerabilities into the IT environment.
Availability Risk – Critical information in the organisation may not be available when needed; this includes risks such as loss of communications (e.g., cut cables, telephone system outage, satellite loss), loss of basic processing capability (e.g., fire, flood, electrical outage) and operational difficulties (e.g., disk drive breakdown, operator errors).
Cloud Strategy and Adoption – The organisation lacks a sufficiently robust cloud strategy and operating model that results in increased costs, reduced system performance, and security or other controls compliance issues.
Confidentiality and Privacy – The organisation lacks sufficient classification and oversight of its data to ensure compliance with applicable regulations, as well as adequate protection and control of data it stores, processes or transmits.
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.
Develop and Maintain the IT Governance Structure – 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 competitors, especially those that are "born digital" and with a low cost base for their operations, or established competitors with superior operations.
Disaster Recovery – The organisation lacks a comprehensive and documented disaster recovery plan or capabilities 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.
Employee Training and Awareness – The organisation lacks a process to determine skills gaps and training needs for IT employees, leading to underperformance with respect to processes, controls/compliance, and the systems environment.

Fit for Purpose – Application systems have inadequate functionality, are not meeting business needs, and involve significant workarounds and/or manual intervention to enable business processes.
Hardware Maintenance Agreements – The organisation has inadequate controls and monitoring of hardware maintenance agreements, which could lead to increased risk of failures and resulting service outages. Unsupported hardware may not be identified for replacement where they are nearing end of support.
Integrity – There is lack of clarity with regard to the authorisation, completeness and accuracy of transactions as they are entered into, processed by, summarised by and reported on by the various application systems deployed by an organisation.
Interface Integrity – Interfaces and data transfer between systems are not appropriately designed, automated, executed or monitored to ensure the integrity of data transferred between systems, including appropriate timeliness of data transfer.
IT Architecture – The organisation's technology architecture is insufficiently designed, deployed and maintained such that it does not meet organisational requirements related to performance, scalability, cost, control or compliance.
IT Asset Management – The organisation lacks sufficient processes to manage IT asset requests, procurement, accounting, deployment, monitoring and retirement.
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 Organisation Change Management – The organisation lacks clear and documented approaches to align, define, adopt and execute dynamic strategies for complex IT changes and transformation.
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.
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.

Project Management Risk – Project management processes are insufficiently mature to ensure consistent delivery of IT projects that meet business needs (including those related to controls and compliance) and to achieve cost and timeline objectives.
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.
Remote Workplace Infrastructure – The organisation lacks sufficient tools, technologies and resources to enable and support a remote workforce for an extended period with necessary levels of control.
Security Incident Management – Security incidents are not identified, classified, routed and tracked to completion. Monitoring and escalation are not defined and/or not effective to ensure incidents are appropriately prioritised and resolved on a timely basis to ensure meeting service requirements and to adequately respond to and recover systems (where appropriate) from attacks and compromises (security).
Service Losses or Disruptions – The organisation is insufficiently prepared for an event that could lead to loss of, or disruption to, the organisation's operations, services or functions; there is not a clear process to identify, analyse and correct hazards to prevent a future re-occurrence.
Shadow IT/End User Computing – The organisation lacks governance, oversight and control over decentrally utilised applications, systems and programs, resulting in business-critical data potentially being at risk due to this data not being managed and protected to appropriate levels.
Software Licensing and Compliance – Inadequate procurement, provisioning, tracking and monitoring controls over software can lead to non-compliance with license obligations (and related penalties) or sub-optimal software license 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.
Strategy and Alignment – The IT organisation is not sufficiently aligned with overall business strategy, including in its projects, operations, people, skills, infrastructure and applications.
Systems Development Life Cycle (SDLC) – Systems development and implementation practices (including design, build, test, deploy activities) are not sufficiently mature to ensure significant system changes and implementations deliver on requirements and have no negative impact to business operations.
Technical Infrastructure/Services – There is not a clear overall process for operating, monitoring and maintaining the organisation's enterprise infrastructure/services to ensure that processing requirements for all business functions are met.
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.
User Access – The organisation's processes related to adding, removing, maintaining and reviewing access rights to digital and information assets are insufficient to prevent violations of segregation of duties and excessive or unauthorised access.

Methodology and Demographics

ISACA and Protiviti partnered to conduct the 9th Annual IT Audit Technology Risks Study in September and October 2020. More than 7,400 (n = 7,470) 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)	5%
IT Executive	3%
IT Risk/Control Executive	2%
IT Audit Director	4%
Audit Director	3%
IT Audit Manager	15%
Audit Manager	6%
IT Manager	6%
IT Risk/Control Manager	10%
IT Audit Staff	18%
Audit Staff	5%
IT Risk/Control Specialist	10%
Other	13%

Type of Organisation	
Private	42%
Publicly traded	38%
Government	13%
Not-for-profit	5%
Other	2%

Industry	
Financial Services – Banking	22%
Government/Education	9%
Technology (Software/High-Tech/Electronics)	8%
CPA/Public Accounting/Consulting Firm	7%
Insurance (except Healthcare Payer)	6%
Tech Services Consulting	6%
Financial Services – Other	5%
Manufacturing (excluding Technology)	4%
Services	3%
Telecommunications	3%
Healthcare Provider	3%
Financial Services – Asset Management	2%
Retail	2%
Power and Utilities	2%
Distribution	2%
Oil and Gas	1%
Transportation and Logistics	1%
Higher Education	1%
Construction	1%
Biotechnology/Life Sciences/Pharmaceuticals	1%
Hospitality	1%
Automotive	1%
Financial Services – Broker-Dealer	1%
Consumer Packaged Goods	1%
Healthcare Payer	1%
Not-for-profit	1%
Chemicals	1%
Real Estate	1%
Media	1%
Airlines	1%
Other	1%

Size of Organisation (other than financial services) – by gross annual revenue in U.S. dollars	
$20 billion or more	15%
$10 billion - $19.99 billion	7%
$5 billion - $9.99 billion	8%
$1 billion - $4.99 billion	17%
$500 million - $999.99 million	11%
$100 million - $499.99 million	15%
Less than $100 million	27%

Size of Organisation (financial services organisations) – by annual assets under management in U.S. dollars	
$250 billion or more	25%
$50 billion - $249.99 billion	11%
$25 billion - $49.99 billion	8%
$10 billion - $24.99 billion	10%
$5 billion - $9.99 billion	9%
$1 billion - $4.99 billion	15%
Less than $1 billion	22%

Organisational Headquarters	
North America	45%
Europe	23%
Asia	18%
Africa	6%
Latin America	3%
Middle East	3%
Oceania	2%

IT Audit Department Headquarters	
North America	45%
Europe	21%
Asia	19%
Africa	6%
Latin America	3%
Middle East	3%
Oceania	3%

Audit Department Headcount	
0-4	18%
5-9	13%
10-19	15%
20-29	9%
30+	45%

Total Number of Full-Time IT Auditors	
0	6%
1	14%
2	12%
3	8%
4	6%
5	8%
6-10	14%
11+	32%

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organisations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organisation that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

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/ISACAGlobal

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 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.

ISACA protiviti®