



Building trust in cloud environments

Fill in what's missing from
your cloud risk strategy

2023 KPMG Cloud Transformation Survey

[kpmg.com](https://www.kpmg.com)

Contents

01 Introduction

02 Research insights

03 Recommendations

04 How KPMG can help

05 Research methodology

06 Authors



01

02

03

04

05

06

Introduction

Don't let a potential lack of stakeholder trust hold back on realizing the potential benefits of cloud deployment

Shifting computing work and data to a cloud environment can alter how companies operate and drive gains in efficiency, agility, resilience, growth, and scale. Cloud adoption has taken off in enterprises of all kinds, as the 2023 KPMG Cloud Transformation survey shows. In the next two years, more than half of the 300 respondents say their organizations plan to host the majority, if not all, of their sensitive data on cloud platforms.

But as enterprises move IT workloads to the cloud, stakeholder distrust is a significant hurdle in taking full advantage of all that the cloud has to offer. From service downtime to sensitive data loss, to audit issues and noncompliance, cloud environments present a range of risks that can have a serious impact on business performance and reputation. Survey respondents name a varied list of public cloud challenges, led by network security and external threats.

The average enterprise in our survey experienced 7.7 business-critical app outages and eight incidents of data loss in the past year. In 87 percent of organizations, auditors or regulatory authorities identified at least two audit issues during that time span.

When stakeholder concerns about cloud risks are not addressed, cloud transformation programs tend to bog down before enterprises realize the full potential value that cloud can deliver. Top management and line of business leaders may deprioritize larger-scale cloud investments. Security, risk and compliance owners may place limits on what data is moved to the cloud. Employees and customers may not take advantage of all the cloud-based tools and services available to them. In this paper, we look at how companies can identify and address security issues as they move more applications and data to the cloud, while enabling stakeholder trust in the transformation.

When stakeholder concerns about cloud risks are not addressed, cloud transformation programs tend to bog down before enterprises realize the full potential value that cloud can deliver.



01

02

03

04

05

06

Eliminate gaps in the cloud risk strategy to realize full value from cloud usage

Our survey shows that companies are moving full-speed ahead with cloud adoption, despite widespread concerns about security and resilience. But as the transition to cloud progresses, enterprises will almost certainly encounter trust issues—one of the most common barriers to cloud transformation success and value realization. As practitioners, KPMG technology risk advisers see this challenge across company types, industry sectors and points along the cloud transformation journey.

In our experience, lack of trust stems primarily from the fact that approaches to monitoring and managing cloud risks are often reactive and decentralized. Many organizations follow enterprise risk frameworks—such as COSO—for designing and integrating internal controls to help assure business processes run in a responsible way that reduces risks and improves performance. Yet, these frameworks do not provide organizations with enough tactical guidance and risk consideration to address and govern risks when moving to the cloud comprehensively. Transitioning to the cloud can present an opportunity to give power and autonomy to departments in the organization. Yet, cloud governance

functions are often inefficient and ineffective at managing the risks created by enterprise-wide and decentralized cloud usage.

Taking complete advantage of all that cloud has to offer demands business, IT, and security leaders address lingering concerns that key data and processes will be secure and resilient in the cloud. KPMG launched the 2023 Cloud Transformation survey to uncover insights about how enterprises can start to achieve this. Our objective revealed the specific elements of a best-in-class approach to cloud risk management, grounded in data-backed insights about what works and what doesn't in the real world.

The main takeaway:

To take full advantage of the promise of cloud technologies, organizations must invest in managing cloud risks across the enterprise and the transformation journey. This report draws on the survey insights and KPMG experience to identify the foundational elements of a leading cloud risk framework and share recommendations for building them.

About the research:

KPMG surveyed 302 senior-level cloud practitioners from a diverse range of organizations about the people, processes, and technologies in place to secure their organizations' cloud environments. The research investigates trends in enterprise cloud risk strategies as well as the operational and compliance outcomes linked to their usage of cloud technologies. We compared how different cloud risk approaches affect how respondents rated their organizations' overall ability to manage cloud risks. We also analyzed the correlation of different cloud risk frameworks to specific risk-related results: incidents of data loss, app outages and downtime, and audit issues. (See the full research methodology, page 20).



01

02

03

04

05

06

Research insights

Cloud adoption and future trends

Key takeaway: Companies are moving more data and systems to public cloud and are increasing the sensitivity of the data involved.

Where are enterprises now, and where are they going next on their cloud journeys? According to this research, more and more organizations are taking to the cloud, with cloud environments becoming an increasingly predominant part of companies' IT.

Seventy-eight percent of all business applications used among our respondent group currently reside in the cloud. Distribution between types of cloud environments is nearly even. Running 30 percent of apps, public cloud infrastructure (IaaS/PaaS) has a slight edge, but also encapsulates more environments. With 26 percent of apps, public cloud SaaS falls just behind, followed by private cloud environments (23 percent).

Where business apps will reside in the future is trending toward public cloud environments. Looking three years ahead, respondents are 28 percent more likely to indicate that their business apps would reside on public cloud versus on-premise or private cloud environments.

Organizations also plan to host more sensitive data in the cloud. Today, 48 percent of all respondents host only a small subset of sensitive data—or none whatsoever—on public cloud. However, in two years' time, 52 percent expect to host

a majority, if not all, of their sensitive data on public cloud. They will also be almost twice as likely to host the majority, or all, of their sensitive data on private cloud within that timeframe.

Exhibit 1. More business applications are moving to public clouds

Question: 36 months from now, approximately what percentage of all your organization's business applications will be run in the following ways?

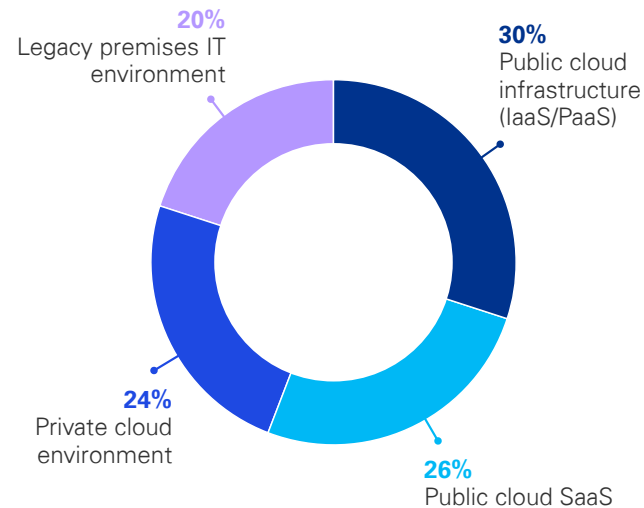
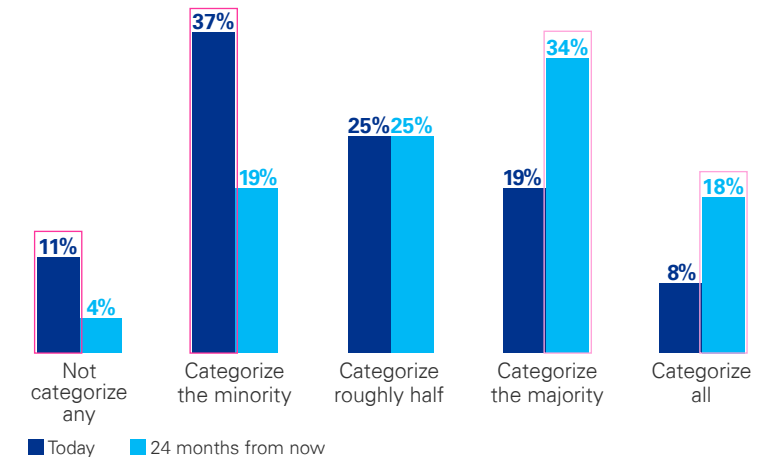


Exhibit 2. Organizations plan to place more sensitive data on public clouds

Question: Approximately what proportion of your organization's public cloud-resident data would you categorize to be "sensitive"?



Cloud risks

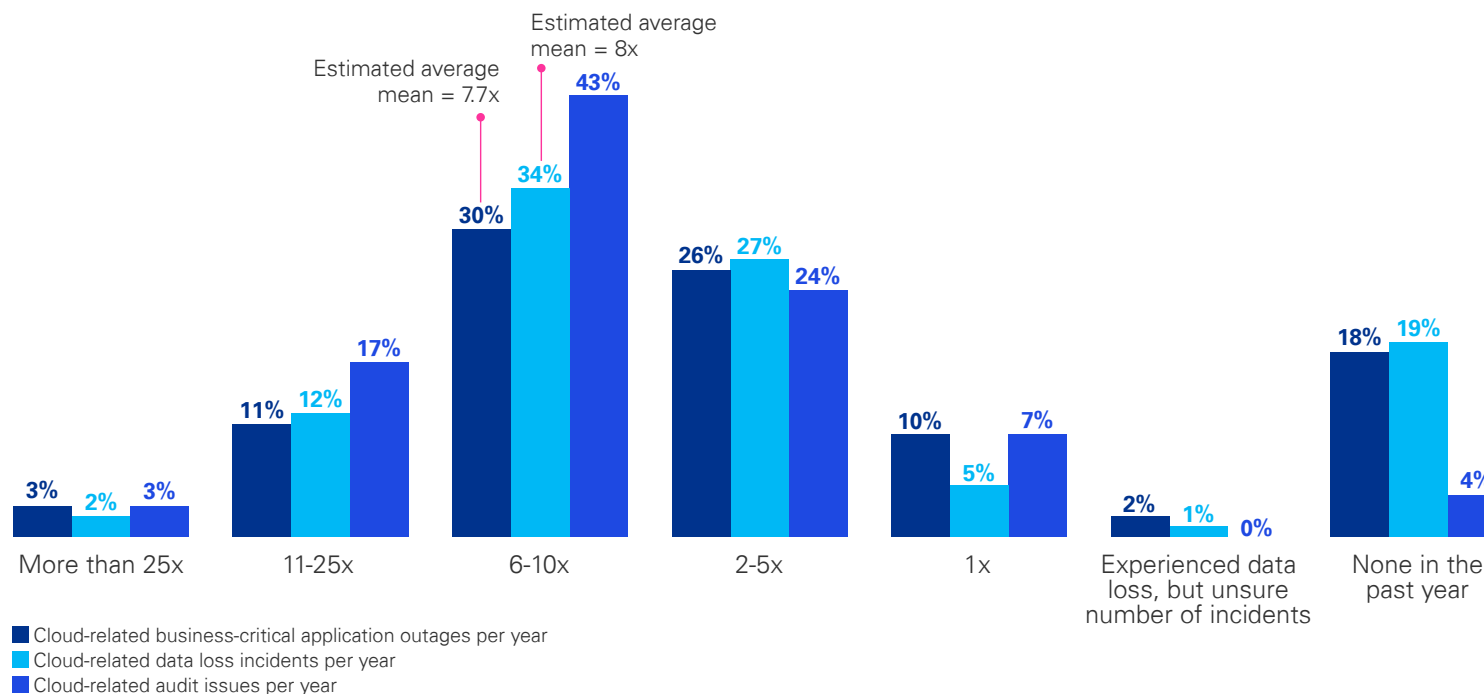
Key takeaway: Enterprises face both new and legacy risks along the cloud migration journey.

While there are differences in risk categories and levels based on the enterprise's cloud usage and maturity, this research indicates that most organizations are looking to strengthen cloud risk management. Barely one in three respondents feel their organization is strong in managing cloud risk, while more than 25 percent describe their organizations' efforts as weak or a work in progress. Even among the respondents that say their organizations have a strong capability for managing cloud risks, the majority (60 percent) say they have not been able to lower the costs associated with cloud risk management. While cloud service providers offer modern and resilient building blocks, organizations still need to architect for operational resilience as part of the shared responsibility model.

The research also shows that moving to cloud is not a magic bullet for operational resilience. More than half of organizations experienced an operational issue in the past year due to cloud risks. IT delays (49 percent), loss of productivity (45 percent), and diminished ability to provide services (45 percent) were the top issues. The estimated average number of data loss incidents was eight. Business-critical application outages occurred an average of 7.7 times.

Exhibit 3. Average annual issues due to cloud risks

Question: Approximately how many times has your organization experienced a business-critical application outage or data loss in the public cloud or had an issue identified by internal auditors, external auditors, or government regulator over the past year?



In the past year, compliance issues due to cloud usage were also prevalent across the respondent pool. Forty-three percent of enterprises had auditors or regulators identify six to 10 issues, and 87 percent had auditors or regulators

identify at least two issues. Cloud user organizations need to bring fresh thinking and evolve their cloud risk management programs rather than lean heavily on legacy IT risk management approaches.

When it comes to using cloud technologies, today's threat landscape is broad, according to the survey findings. Respondents are concerned about a wide variety of internal and external threats, led by: malware moving laterally to cloud workloads (36 percent); attacks that result in the loss of data due to the insecure use of APIs (32 percent); and unauthorized access by a third party (32 percent). Cloud is not merely an extension of the data center, meaning the traditional protection applied to on-premises data center infrastructure is not sufficient.

Public cloud environments pose particular risks due to shared responsibilities for securing both information and access. Network security (27 percent) is at the forefront of a long list of public cloud risk concerns. Other top challenges organizations face in protecting their public cloud workloads are application security (24 percent), managing cyberattacks (23 percent), and data loss and leakage (22 percent).

Exhibit 4. Today's cloud threat landscape is broad

Question: Which of the following threats/incidents is your organization most concerned about today as it relates to your organization's use of cloud technologies? (multiple responses accepted)

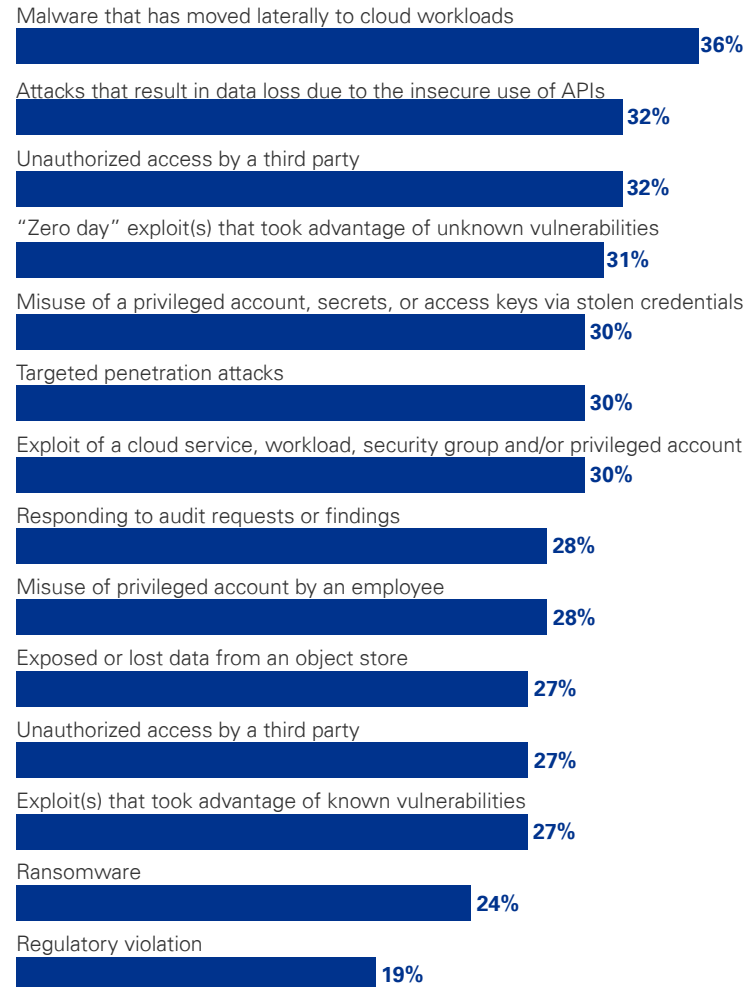
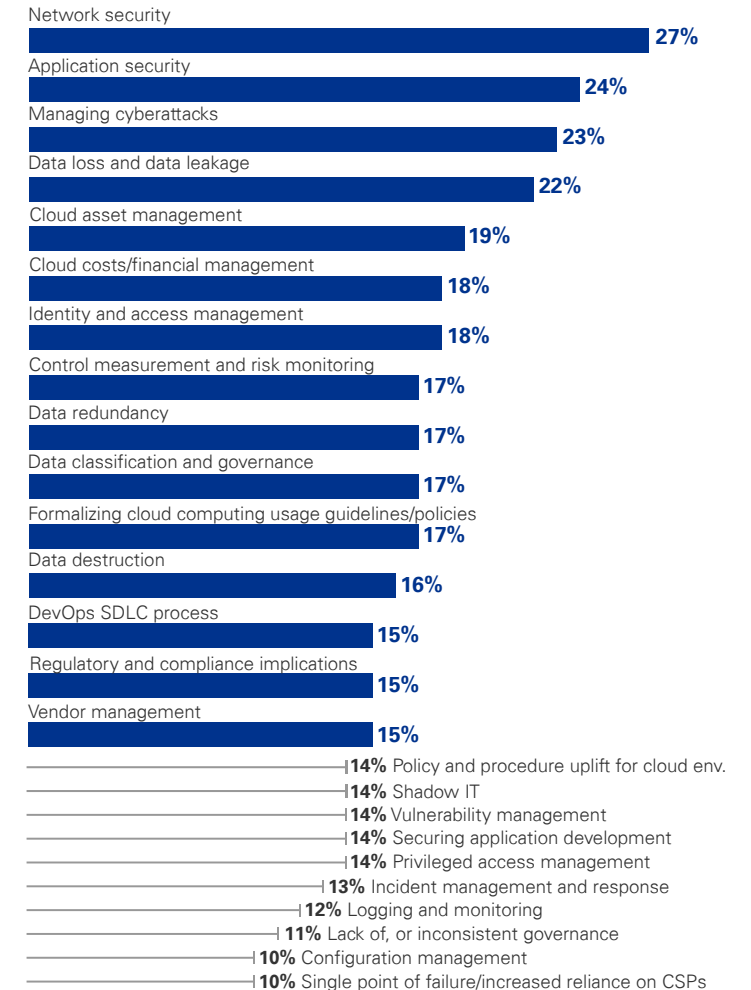


Exhibit 5. Network security and external threats lead a long list of public cloud challenges

Question: Given your organization's current experience level and public cloud use cases, which of the following areas of risk are most problematic or challenging? (five responses accepted)

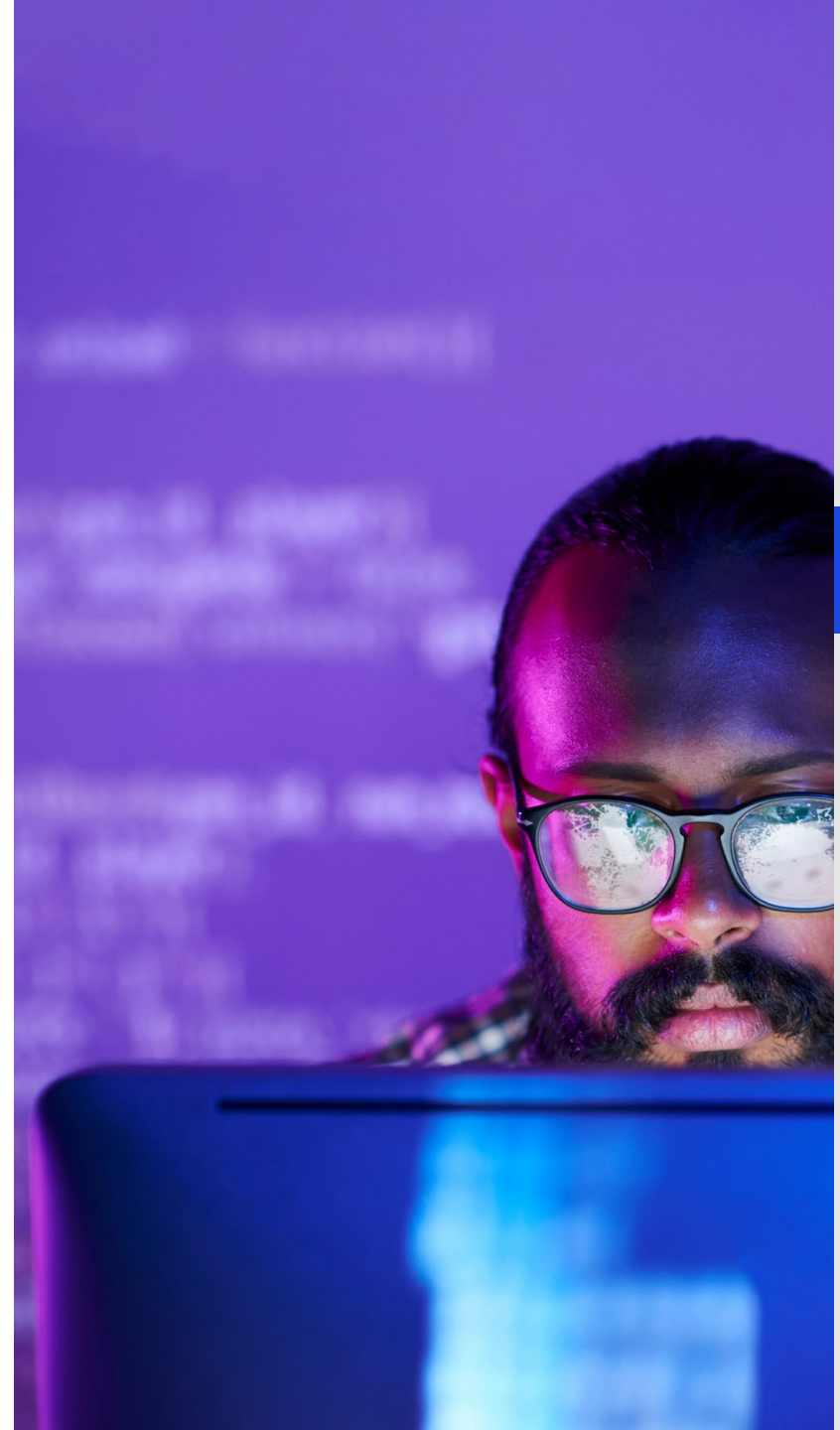
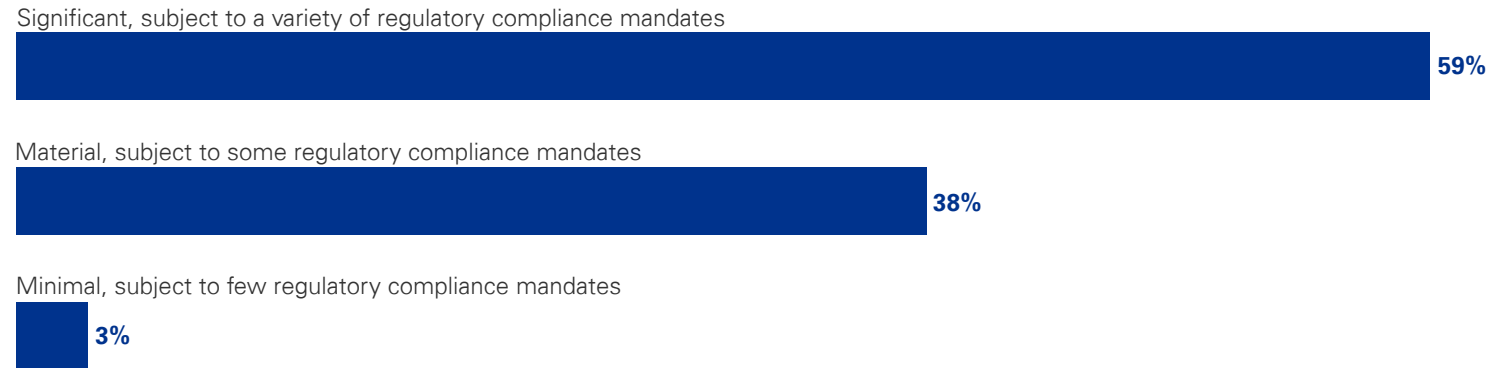


Regulatory issues also pose risks as organizations adopt cloud technologies. Nearly six in ten respondents (59 percent) say their organizations' regulatory exposure and commitments are significant, and they are subject to a variety of compliance mandates. A notable portion of the survey

population also indicated that cloud usage makes compliance with all regulations and requirements more complicated with Europe's General Data Protection Regulation (GDPR) the biggest challenge, selected by 35 percent of respondents.

Exhibit 6. Regulatory exposure/commitments are significant

Question: How would you generally describe your organization's regulatory exposure/commitments?



01

02

03

04

05

06

Cloud risk management approaches

In our survey, we asked IT and security leaders what factors were most important to building a successful cloud risk management process. Here are some of the top insights they provided.

There is a strong correlation between proactive risk management and improved cloud outcomes.

Key takeaway: Early, hands-on cloud risk management leads to fewer incidents, with smaller impacts, at lower costs.

This research shows a strong correlation between proactive risk management and improved cloud outcomes. Companies that took a proactive approach (rather than reactive) to cloud risk management scored more highly on favorable KPIs and were 2.3 times as likely to rate their ability to manage cloud-risk as “strong.”

The most proactive cohort is more successful than the other cohorts in:

- Aligning with relevant industry frameworks
- Meeting application uptime and performance SLAs
- Proving compliance
- Protecting against data theft, loss, and unauthorized access

Exhibit 7. Companies that were most proactive about cloud security are twice as likely to say their security is strong

Question: How would you rate your organization’s ability to manage cloud risk?

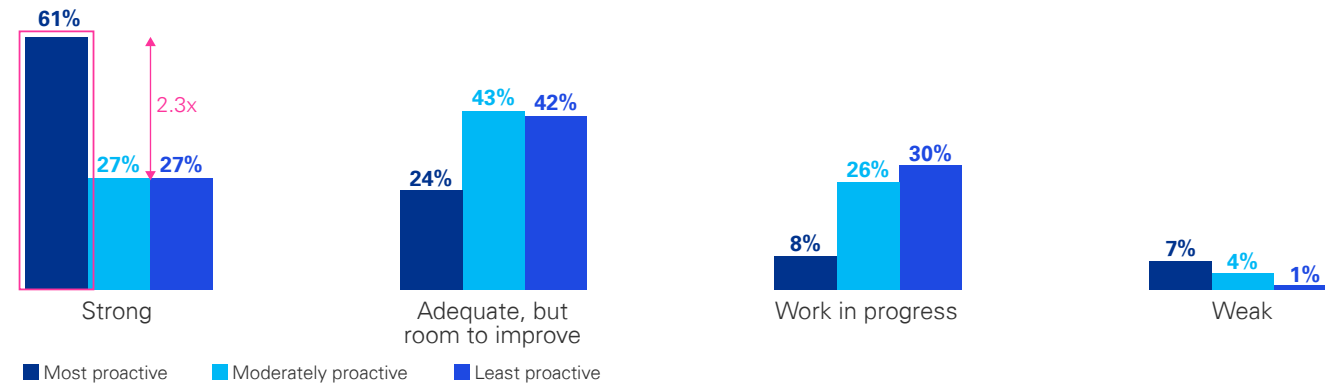
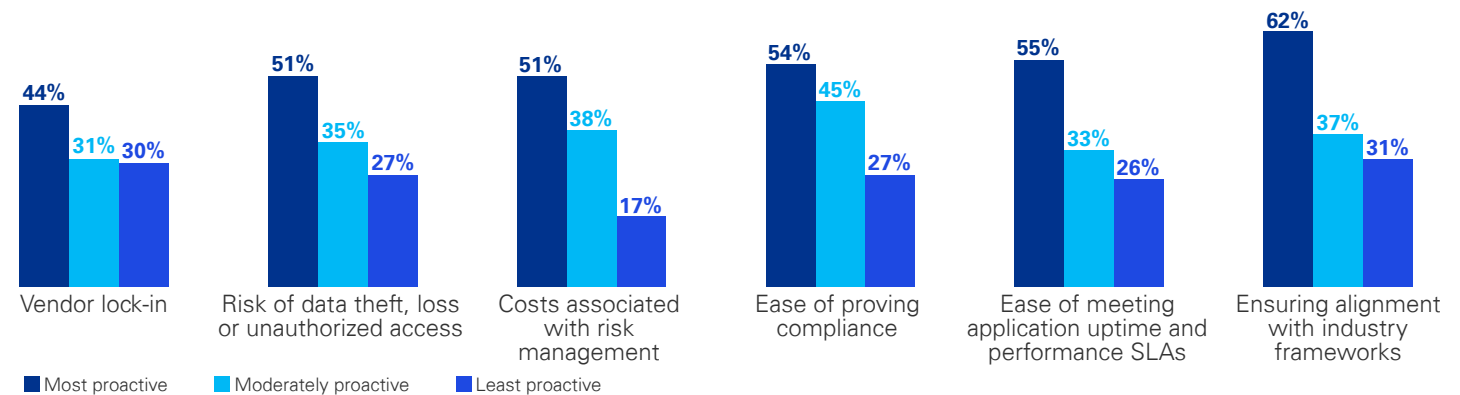


Exhibit 8. More proactive cloud risk managers were more successful across the board

Question: How has your organization’s use of cloud services impacted each of the following? (Percent of respondents selecting “Significantly improved”)



01

02

03

04

05

06

In three important areas, the most proactive cohort sees especially strong results. Organizations that are more proactive in risk management when adopting cloud services indicated that they were more likely to see significant improvements in the costs around risk versus those companies that are more reactive. It is also 48 percent are more likely to have significantly improved their experiences and issues with vendor lock-in. Finally, the most proactive cohort is 75 percent more likely to have a short recovery time from cyberattack—experiencing a mean time to recover (MTTR) between 1 and 59 minutes—than other cohorts.

In contrast, the least proactive cohort struggles to deal with certain cloud risks. For example, it is 72 percent are more likely than the most proactive cohort to have lower confidence navigating a cyberattack.

Exhibit 9. Proactive cloud risk managers are more likely to see improvements in risk management costs

Question: How has your organization's use of cloud services impacted costs associated with risk management?

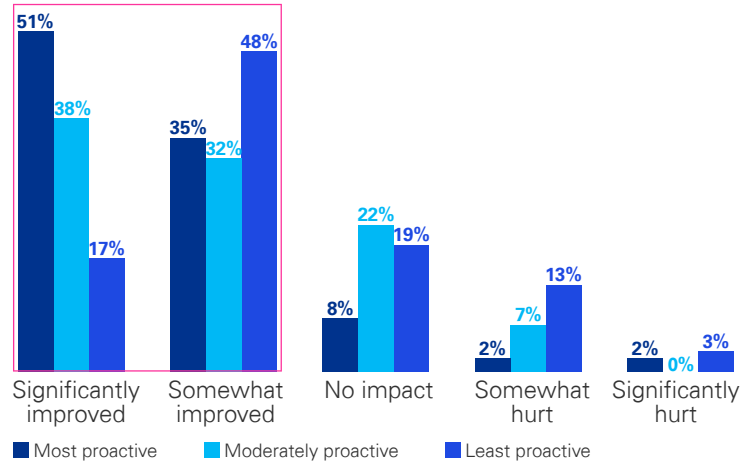


Exhibit 10. Proactive risk managers have less difficulty with vendor lock-in

Question: How has your organization's use of cloud services impacted each of the following?: Vendor lock in (e.g., potential difficulty migrating data/applications out of a CSP's environment in the future).

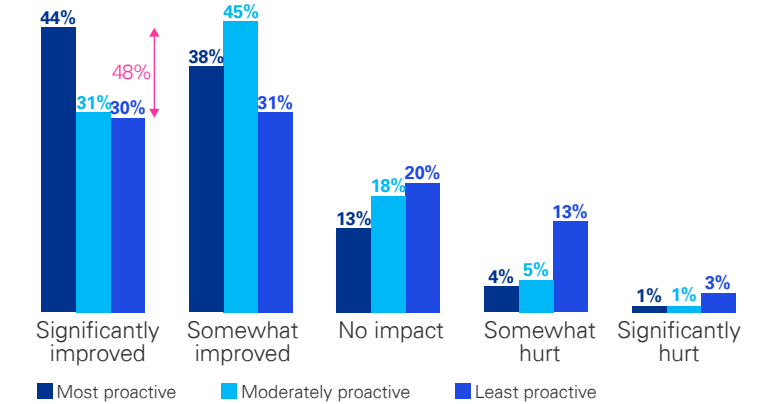
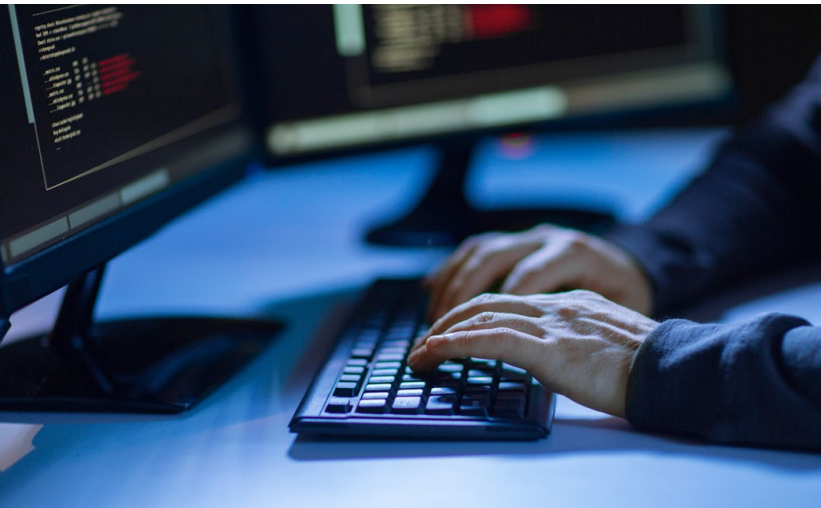
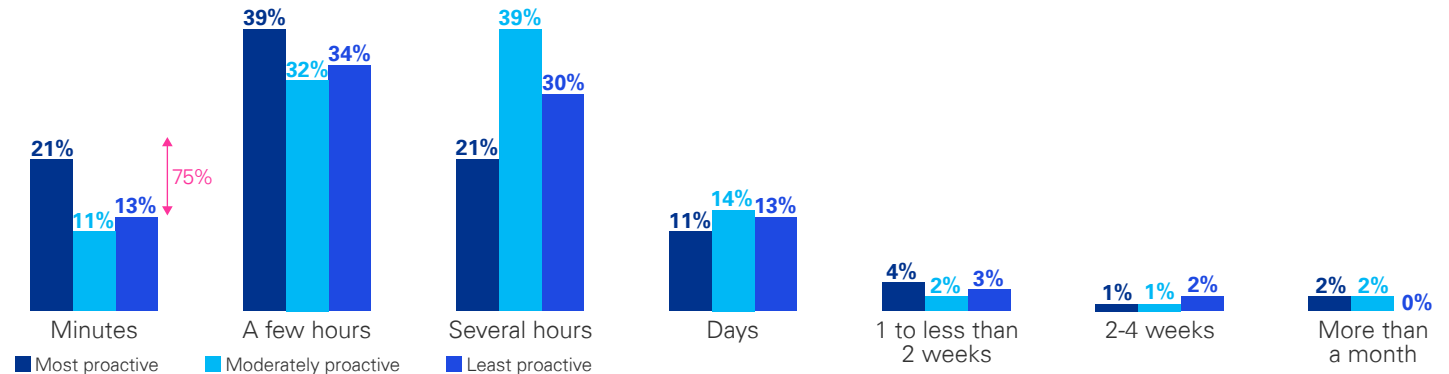


Exhibit 11. The most proactive risk managers are 75% more likely to have the shortest recovery time from app outages due to cyberattack

Question: Generally speaking, what is your organization's mean time to recover (MTTR) for business-critical applications suffering from unplanned downtime tied to a cybersecurity attack?



01

02

03

04

05

06

Empowering people throughout the enterprise can be a key success factor.

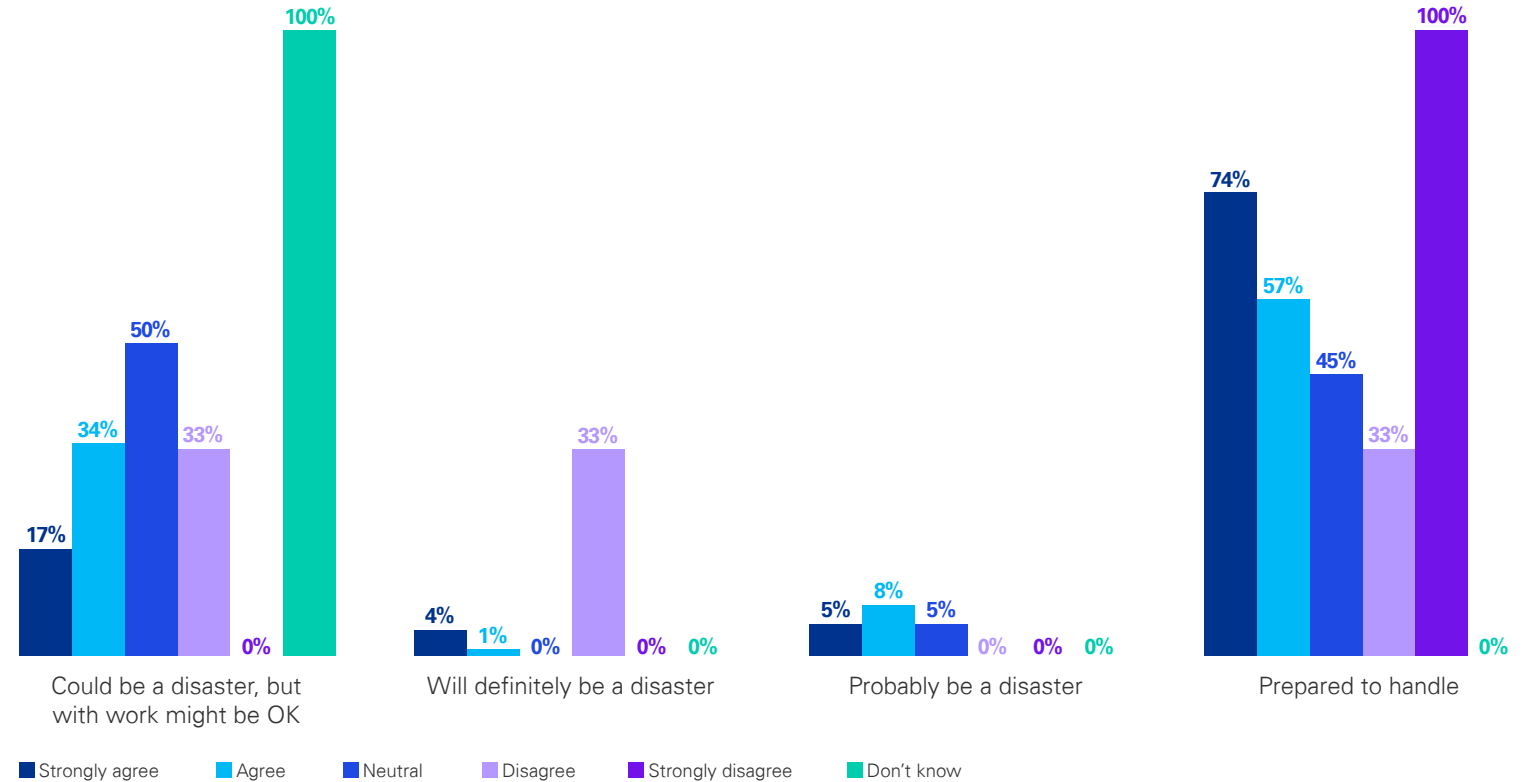
Key takeaway: When it comes to cloud risk management, enterprises with higher rates of cross-functional cooperation, employee training, and middle manager engagement report greater preparedness and outcomes.

This research indicates that cross-functional cooperation across the organization drives better cloud risk outcomes. As the perception of preparedness increases in our respondent group, so does the emphasis on both cross-functionality and consensus on risk management. Cross-functional cooperation is important because cloud products can be adopted relatively easily without it. As such, effective risk management requires perspectives and inputs of multiple groups—IT, legal, procurement, third-party risk management, and information security—similar to how enterprises approach adoption of traditional technology and computing.

Exhibit 12. Better prepared risk managers emphasize cross-functionality and consensus

Question 1: Rate your level of agreement with the following statement: The nature of cloud services is such that managing risk effectively demands cross-functional focus and buy-in on risk management.

Question 2: What is your mindset when a cyberattack is uncovered by your organization's security team affecting public cloud-resident data or applications?



Second, cloud risk management driven by middle management tends to drive success. The data shows that middle management responsibility for cloud risk correlates to higher confidence in cyberattack preparedness and ability to manage cloud risk. We also see middle management becoming more involved as incidents increase, as they are more in tune with day-to-day operations. Specifically, as the numbers of data loss incidents and app outages increase, the more likely risk management strategies are to be developed in middle management.

Finally, employees across the organization need to be well-trained. According to the research, more training correlates to a better ability to manage cloud risk. As resilience increases, so does training. Higher-trained staff members are more likely to identify the continued need for training.



Exhibit 13. Companies with rising losses focus on middle-out cloud risk management strategy development

Question 1: Regardless of the functional groups involved, which best describes how your organization develops risk management strategies for cloud environments?

Question 2: Approximately how many times has your organization experienced data loss in the past year specifically related to its public cloud-resident data?

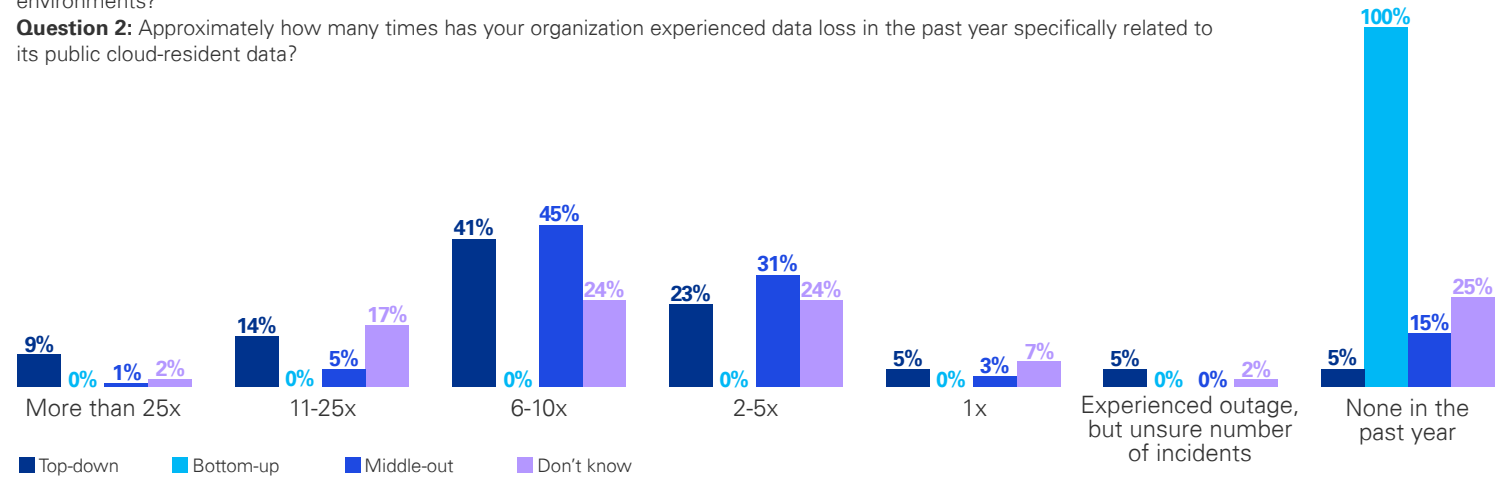
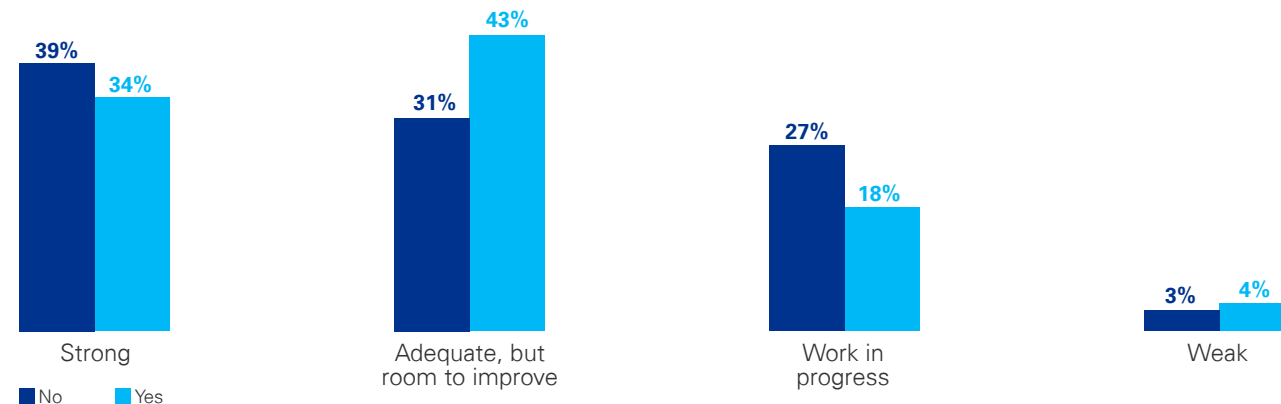


Exhibit 14. More employee training correlates to stronger cloud risk management

Question 1: Which of the following measures has your organization prioritized that have had the greatest impact in improving the risk associated with your organization's use of cloud services?

Question 2: How would you rate your organization's ability to effectively manage cloud risk?



Frameworks and standards can help set companies on the right path.

Key takeaway: Companies improve cloud risk confidence by leveraging industry standards.

Although there is no one-size-fits-all approach for managing cloud risk, it can be helpful to have a prior plan to get behind. That's where technical and industry-agnostic risk frameworks for cloud can help. According to the data, companies improve cloud risk confidence by leveraging industry standards.

The research shows a correlation between leveraging industry frameworks/standards and increased incident numbers: As the number of data loss incidents among the respondent group increases, so does the enterprise's likelihood to leverage industry standards to guide risk assessment. Our view is that fear of incidents drives enterprise focus on leveraging frameworks.

Leveraging industry frameworks and standards also correlates to higher confidence in cyberattack preparedness and ability to manage cloud risk, our survey shows.

Frameworks provide a common comprehensive list of potential risks for organizations to leverage as a starting point. Primary risk and control frameworks include the Cyber Risk Institute (CRI)'s Cloud Profile framework, the Cloud Security Alliance (CSA)'s Cloud Controls matrix, and Guidelines on Security and Privacy in Public Cloud Computing (NIST SP 800-144), while notable technical standards and frameworks include Center for Internet Security (CIS) Benchmark and technical security configuration guidance provided by the cloud service providers.

Exhibit 15. The more organizations leveraged industry standards, the greater the confidence in their cloud risk management

Question 1: Does your organization currently leverage any industry frameworks/standards to benchmark, measure, and control cloud risk?

Question 2: How would you rate your organization's ability to effectively manage cloud risk?

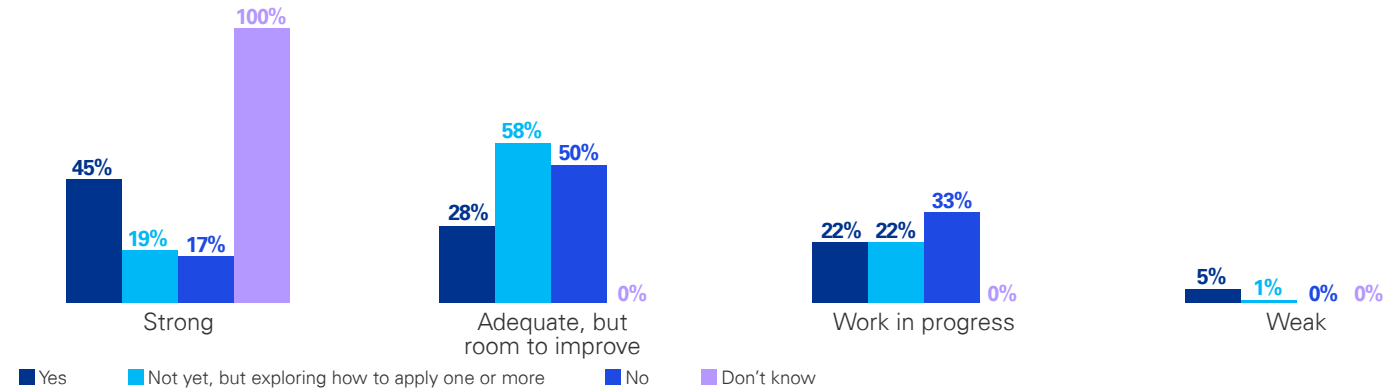
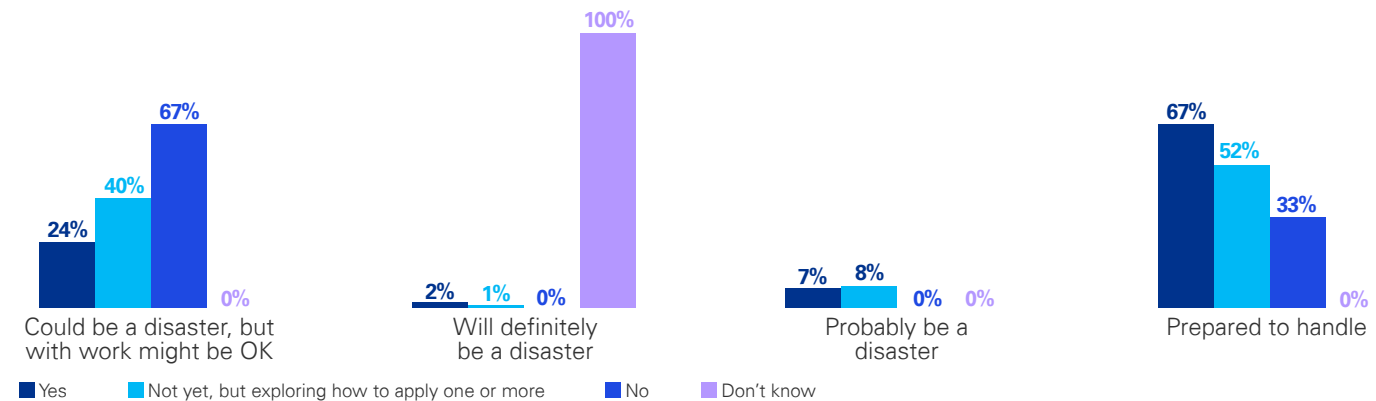


Exhibit 16. Application of industry standards correlates with greater confidence in cloud cybersecurity

Question 1: Does your organization currently leverage any industry frameworks/standards to benchmark, measure, and control cloud risk?

Question 2: What is your mindset when a cyberattack is uncovered by your organization's security team affecting public cloud-resident data or applications?



Third-party experts can help corral resources and prioritize activities

Key takeaway: Companies improve cloud risk confidence by leveraging industry standards.

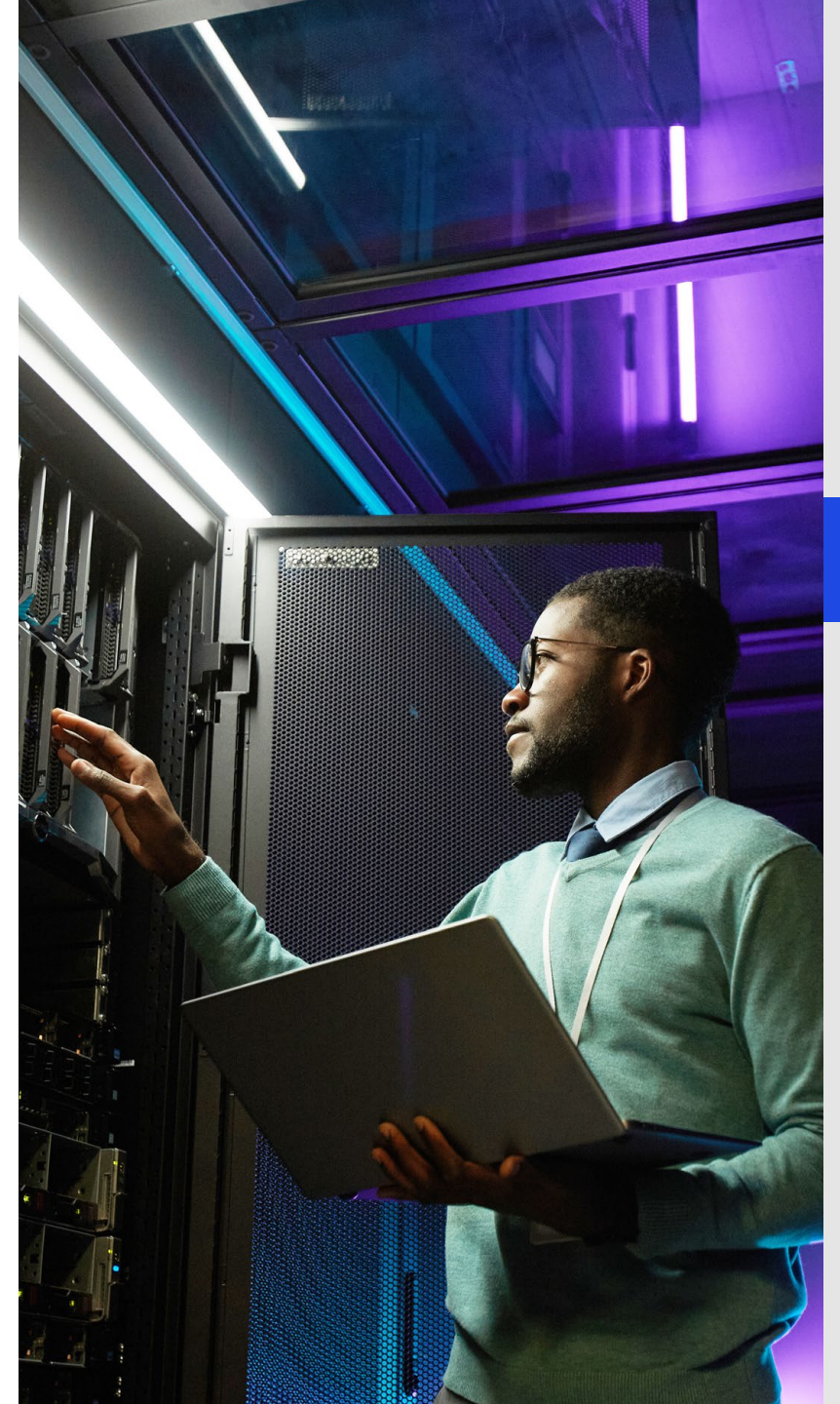
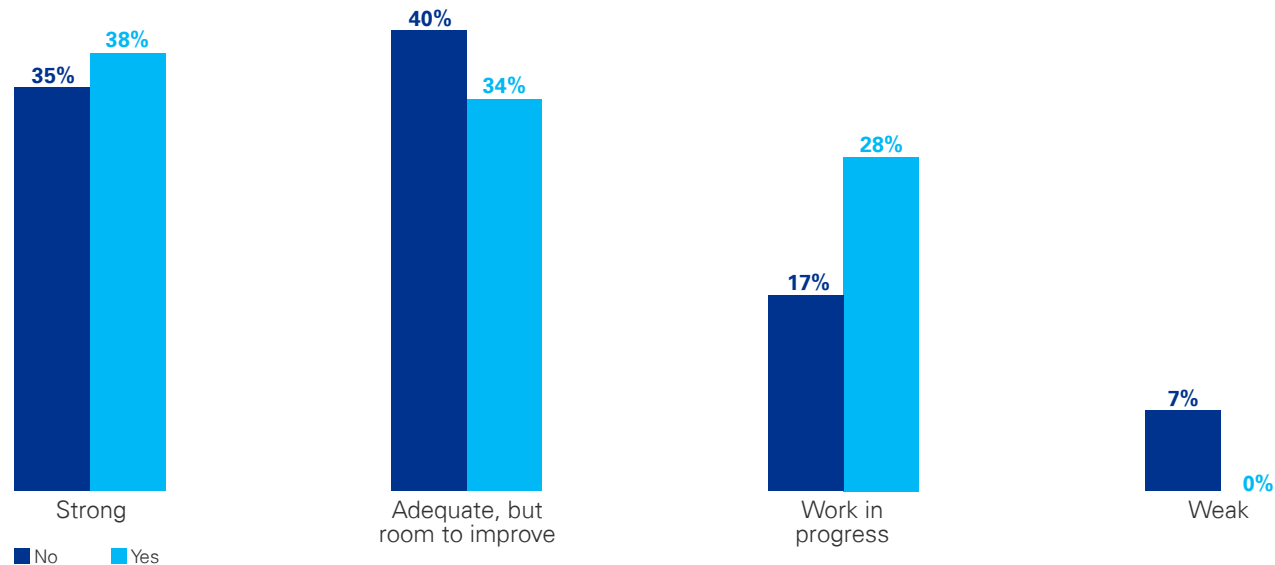
Managing cloud risk should be a collaborative endeavor. Given the complexity of cloud environments and speed of technological change, a third-party consultant can drive

considerable value. The research shows that engaging consultants for cloud risk management services improves companies' ability to manage cloud risk, likely due to the consultants' experience with other companies in the same industry and knowledge of leading practices.

Exhibit 17. Companies that engage third-party risk management services are more confident in their cloud security

Question 1: Which of the following measures has your organization prioritized that have had the greatest impact in improving the risk associated with your organization's use of cloud services?

Question 2: Generally speaking, how would you rate your organization's ability to effectively manage cloud risk?



01

02

03

04

05

06

Recommendations

Essential pieces of a leading cloud risk framework

Our in-depth analysis of the survey findings—along with our own proficiency and experience in leading cloud transformation programs in a diverse range of organizations—allows us to identify common elements of effective approaches for managing the complex and evolving array of risks in the cloud. Together, they provide strong, data-backed evidence of the power of a comprehensive cloud risk framework that integrates operational and governance capabilities for continual security, resilience and compliance of products, services and workloads running in the cloud. Organizations that embrace such an approach are most successful at reducing risks in cloud environments while improving cloud-based business process performance. They rated their ability to manage cloud risk the highest and also experienced fewer operational incidents and audit issues.

We offer recommendations for organizations seeking to improve their cloud risk outcomes, to fill in the four missing pieces in their cloud operating models.

01 **Develop a cloud strategy and vision that balances business and risk and compliance objectives.**

Design a coherent strategy for moving to the cloud and define policies, procedures, and guidance for managing risks, while keeping the broader objective top of mind.

- Maintain continuous alignment between the use of cloud services with the organization's strategic objectives and integrate the cloud journey with the IT strategy.
- Document cloud governance and security standards to strengthen oversight.
- Define roles and responsibilities to create accountability for managing risk in the cloud journey.
- Align on a clear business case with value drivers for the cloud journey that includes key risk considerations.

02 **Implement a unified and collaborative cloud governance approach between business, IT and risk management.**

Bring together technology, business, and risk teams to plan, prepare, and take steps to ensure the cloud migration meets the needs of the organization and minimizes risk.

- Define and configure the migration plan, applications, and infrastructure for stronger security.
- Review and evaluate regulatory compliance considerations such as SOX, GDPR, HIPAA, and other data confidentiality and privacy laws to ensure compliance objectives are met.
- Document cloud governance and security standards for moving systems to the cloud and strengthen oversight of systems in the cloud.
- Incorporate a controls workstream for each migration to the cloud that ensures appropriate controls are implemented prior to cloud deployment.
- Implement and maintain the cloud control environment to prevent unauthorized access and connections to improve operational performance and stability.

03

Establish proactive and agile cloud risk management.

Agility is paramount to optimize business value and support the business strategy in a quickly growing cloud environment. This will require commensurate agility in cloud risk management. Establish mature processes to ensure applications and data are securely migrated to the cloud environment the first time, and every time. Operate and optimize cloud operations using preventative and detective controls within the cloud environment to meet security and compliance objectives throughout the cloud journey.

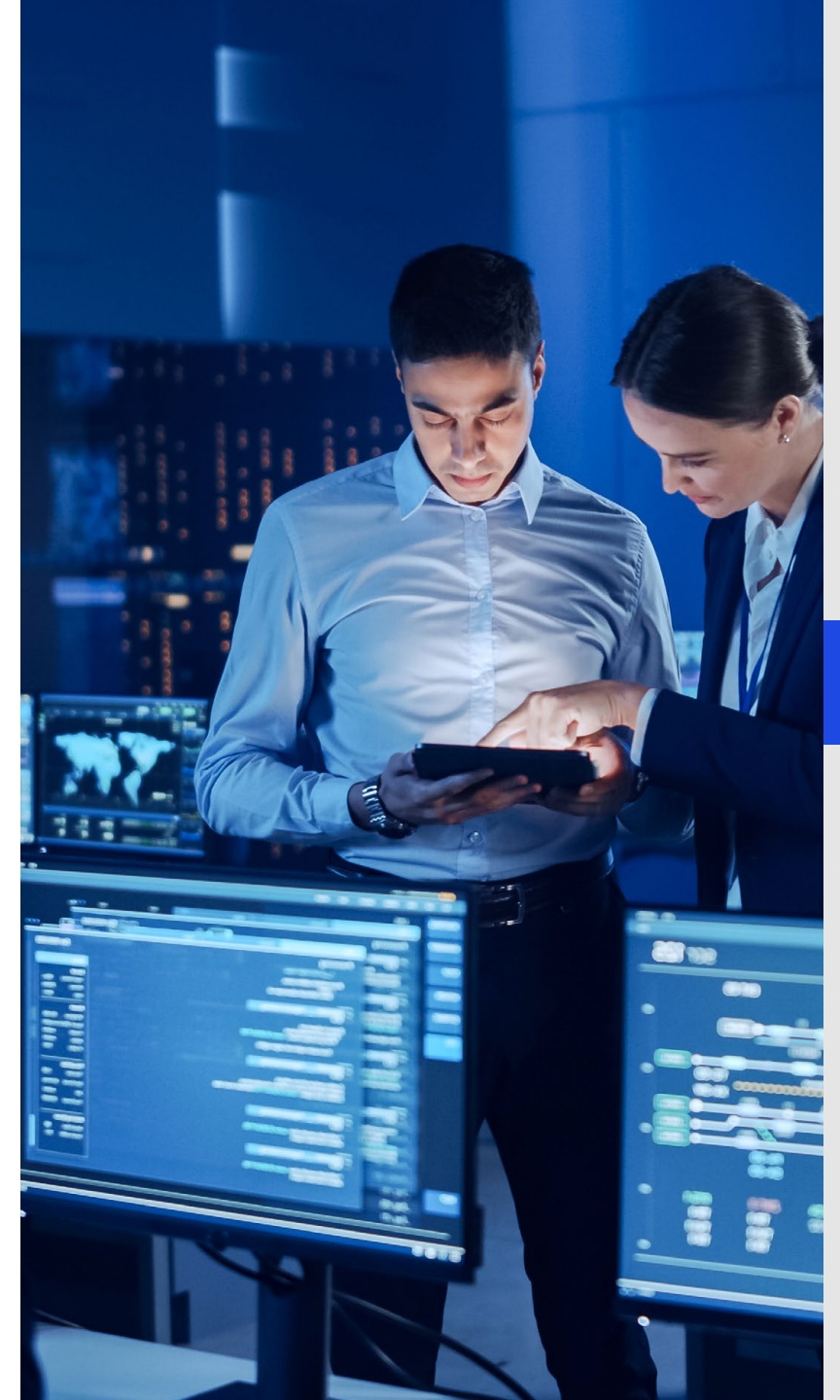
- Setup controls to ensure applications and their data are migrated completely and accurately to the cloud, preventing data loss and unintended system downtime.
- Appropriately configure the cloud infrastructure to secure confidential data, and have appropriate measures in place for your most sensitive data.
- Establish strong processes to grant and monitor cloud access rights throughout your cloud journey to ensure that access to cloud resources is commensurate with job responsibilities.

04

Leverage cloud provider risk management capabilities.

Most cloud providers offer basic risk management functionalities as part of their cloud management suite, as well as add-ons and bolt-ons available for an extra cost, which make risk monitoring more viable and feasible. Companies can also integrate their existing risk management tools with those of their cloud providers to get a more holistic perspective on risk, in a customized way that works best for their cloud operations' vision, strategy and structure.

- Identify, deploy, and use tools available from cloud providers to support and strengthen cloud risk management efforts already taking place within business units.
- Start this evaluation and integration early. With the rapid adoption of the cloud, it will give companies a head start—and make a meaningful difference—in achieving effective cloud risk management.



01

02

03

04

05

06

How KPMG can help

Operating effectively in the cloud may require enterprises to strike a careful balance between business needs and risk and compliance goals. KPMG can help organizations design and implement a leading-edge cloud operating model, including governance and risk management through the end-to-end cloud journey.

The KPMG Cloud Target Operating Model provides a new way of thinking about the people, tools, and processes involved in managing cloud risks. Driven by each individual company's cloud vision and strategy, it helps organizations deliver increased business value from their cloud environment while building trust in cloud-based products and services through assured security, resilience, and continual compliance.



Cloud transformation: Cloud controls uplift

KPMG helped a leading financial services company uplift its controls during its cloud migration journey.

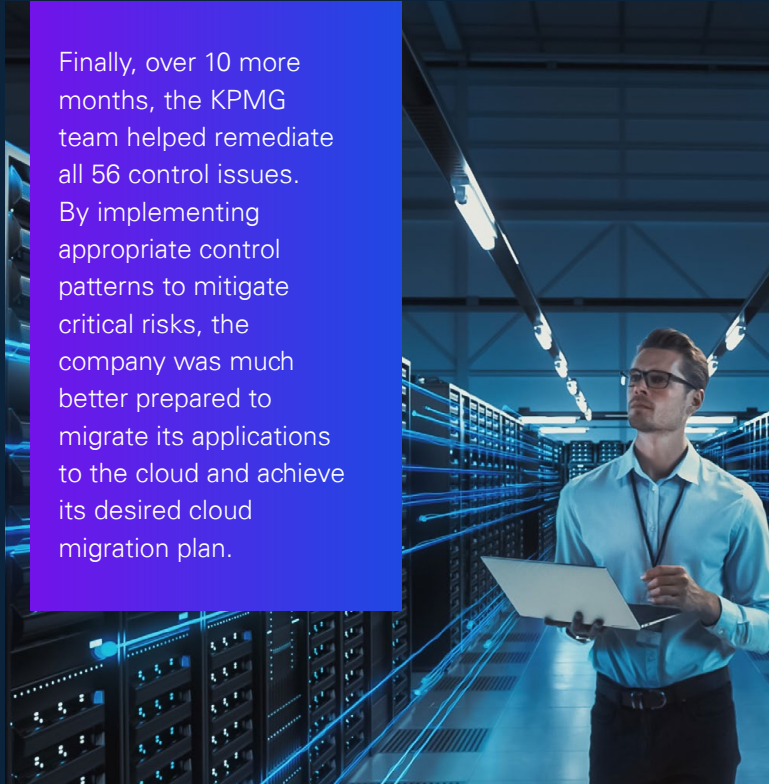
To achieve productivity, cost efficiencies, and speed of delivery, a leading financial services company planned to migrate its on-premises applications to the Amazon Web Services (AWS) cloud computing platform. The cloud transformation journey was likely to introduce a wide range of governance and compliance risks, requiring the company to assess the readiness of its enterprise control activities to support its migration to cloud.

The company engaged a team of KPMG cloud, security, and risk professionals to help improve its readiness posture by proactively identifying risks and control concerns associated with the applications' move to AWS. This required a comprehensive understanding of the company's cloud environment, the data and applications being stored and processed in the cloud, and the regulatory requirements that apply to the organization.

First, the KPMG team designed a template for cloud controls mapping, using inputs from various industry frameworks, regulatory and compliance requirements, and industry standards.

Next, focusing on all tools and systems used within the company's end-to-end control process, the KPMG team reviewed and tested key control points over a five-month period. Through this work, the KPMG team identified 56 potential concerns, which include the following:

- Platform access was not integrated with firm strategic tools for access request, approval, and recertification processes.
- Privileged access was not detected and monitored to ensure appropriate management within the firm privileged access management tool.
- Changes made to production did not go through strategic change deployment tools to ensure the appropriate testing and approval.
- A critical production process was not monitored and alerted for incident resolution.



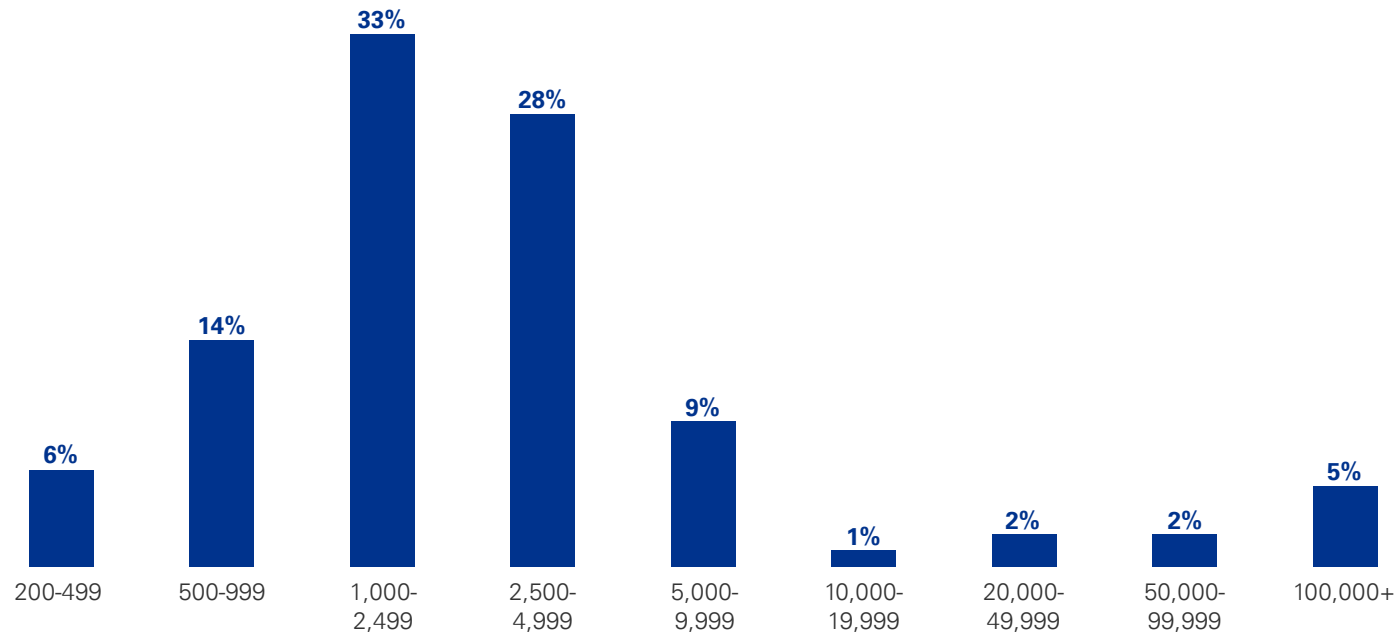
Finally, over 10 more months, the KPMG team helped remediate all 56 control issues. By implementing appropriate control patterns to mitigate critical risks, the company was much better prepared to migrate its applications to the cloud and achieve its desired cloud migration plan.

Research methodology

The insights in the report are based on responses to an online survey by KPMG and Enterprise Strategy Group in September-October 2022. Respondents include 302 information security, information technology, risk and compliance, technology, and internal audit professionals with a high degree of knowledge about the people, processes, and technologies in place to secure their organizations' cloud environments.

Respondents by number of employees

Question text: How many total employees does your organization have worldwide? (Percent of respondents, N=302)



To realize value from cloud environments, companies need a comprehensive cloud risk framework that integrates operational and governance capabilities for continual security, resilience and compliance of products, services and workloads.



01

02

03

04

05

06

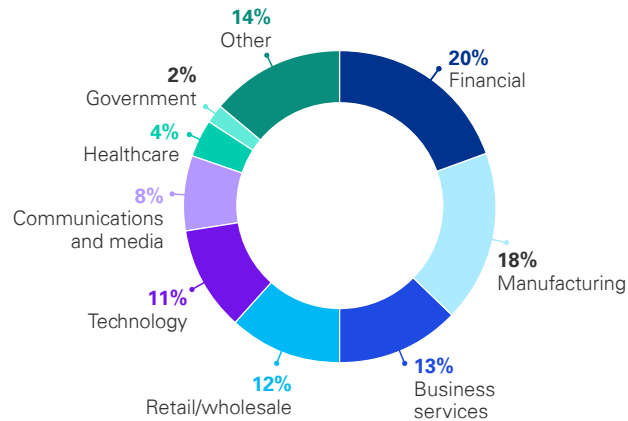
Approach to survey data analysis: To understand relationships between cloud risk management approaches and outcomes within the survey population, our data analysts took two primary approaches to analysis.

- We segmented the full survey population into three cohorts based on how they rated their organizations' cloud risk management proactiveness across three areas:
 1. Defining new policies for the cloud service
 2. Working with the cloud service provider to address ambiguities about shared responsibilities
 3. Adopting security controls for the cloud service

- Organizations that did not select "always proactive" in any areas are named "least proactive;" organizations that selected "always proactive" in one area are named "moderately proactive;" and organizations that selected "always proactive" in two or three areas are called "most proactive."
- We also compared significant relationships between cloud risk outcomes (responses to questions about app outages, data loss incidents, and audit issues, as well as ratings of cloud risk preparedness and confidence) and cloud risk approaches (questions about cloud risk management organizational structures, processes, policies and people).

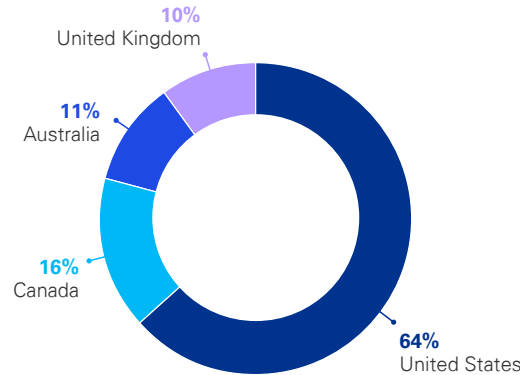
Respondents by industry

Question text: What is your organization's primary industry?
(Percent of respondents, N=302)



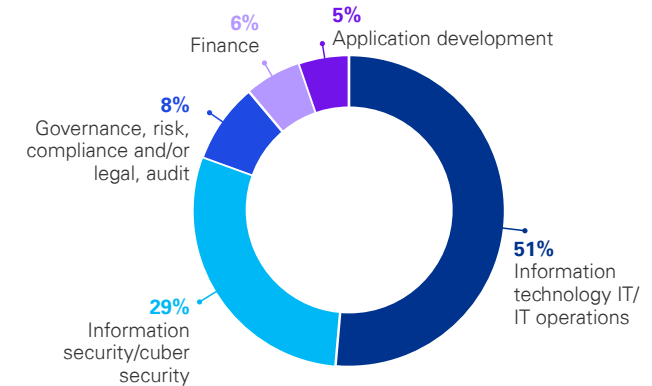
Respondents by country

Question text: (Percent of respondents, N=302)



Respondents by job function

Question text: Which of the following describes your current job function?
(Percent of respondents, N=302)



01

02

03

04

05

06

Authors



Emily Frolick

*Partner,
U.S. Trusted Imperative Leader*
efrolick@kpmg.com



Sai Gadia

*Partner,
Cyber Security Services*
sgadia@kpmg.com



Bindiya Khurana

*Principal,
Technology Risk*
bkhurana1@kpmg.com



Sachin Satija

Principal, CIO Advisory
sachinsatija@kpmg.com



Michael Bruner

*Managing Director,
Internal Audit & Enterprise Risk*
mbruner@kpmg.com



Lavin Chainani

*Managing Director,
Technology Risk*
lchainani@kpmg.com



Christian Leva

*Managing Director,
GRC*
cleva@kpmg.com



Craig Hays

*Managing Director,
Digital Lighthouse*
craighays@kpmg.com

With special thanks to:

Barry Brunsman for his contributions and insights in this report.



01

02

03

04

05

06

For more information, please contact:

Emily Frolick

*Partner,
U.S. Trusted Imperative Leader*

KPMG LLP

+1 513 763 2453

efrolick@kpmg.com

Related thought leadership:



2022 KPMG U.S.
Technology Survey Report



The Trusted Imperative



2022 KPMG U.S. CEO Outlook

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



kpmg.com/socialmedia

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

DASD-2023-12610



01

02

03

04

05

06