Measuring Risk and Risk Governance

cloud security alliance®

Acknowledgments

Lead Authors:

Hillary Baron
Catherine Nelson
Chris Rezek
John Yeoh

Contributors:

Josh Buker
Alex Kaluza
Etienne De Burgh
Taylor Lehmann
MK Palmore
Nick Godfrey
Phil Venables

Designers:

Claire Lehnert
Stephen Lumpe

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, training, certification, events, and products.

Table of Contents

Survey Creation And Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA is also tasked with educating various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys help gauge the maturity of information security technology at various points in the industry, as well as the rate of adoption of security best practices.

Project sponsors are CSA Corporate Members who support the findings of the research project. CSA has full content development and editing rights of the research.

The goal of this research project is to assess the maturity of public cloud and risk management within the enterprise. The key areas of interest include:

- Understand current challenges and perceived effectiveness of risk management in public cloud
- Understand the impact of effective risk management practices in the cloud
- Identify best practices to reduce risk and address risk tolerance in the cloud

Google partnered with CSA to develop a survey to add to the industry's knowledge about enterprise risk and to prepare this report of the survey's findings. Google co-developed the initiative by participating with CSA in the development of survey questions addressing methods for measuring risk and risk governance. The research was conducted in two phases:

- **Phase 1**: A series of interviews were conducted by CSA from April to June 2021 based on an initial set of questions. Respondents were asked to fill out a survey and discuss their responses in detail during the interview. Data were analyzed and used to refine the question set.

- **Phase 2:** The refined set of questions was used to conduct an online survey by CSA from July to August 2021. Over 600 responses were received from IT and security professionals from a variety of organization sizes and locations. Data analysis was performed by CSA's research team.

The survey report is based on the perceptions and opinions of 20 executive interviews and 600 security practitioner surveys collected by CSA in 2021. Researchers, analysts, and industry experts within the CSA community present the following observations and statistical correlations from the data collected and existing knowledge on risk management and measurement in the cloud.

Executive Summary

The process of digital transformation involves adopting technologies that enhance operational and customer experiences. Moving to the cloud represents this transformation, often upgrading the organizational approach to application, data, and infrastructure security. Enterprise risk assessment processes must now adapt to the cloud model and consider the implications of the shared responsibility model, where both the Cloud Service Provider and customers have ownership in the delivery of services. The COVID-19 pandemic has added another element, accelerating the use of such tools and services, causing risk management practices to adapt quickly to the cloud adoption model. As the reliance on cloud services increases, Enterprise risk management processes must evolve at the required pace of the cloud to maintain and improve efficacy.

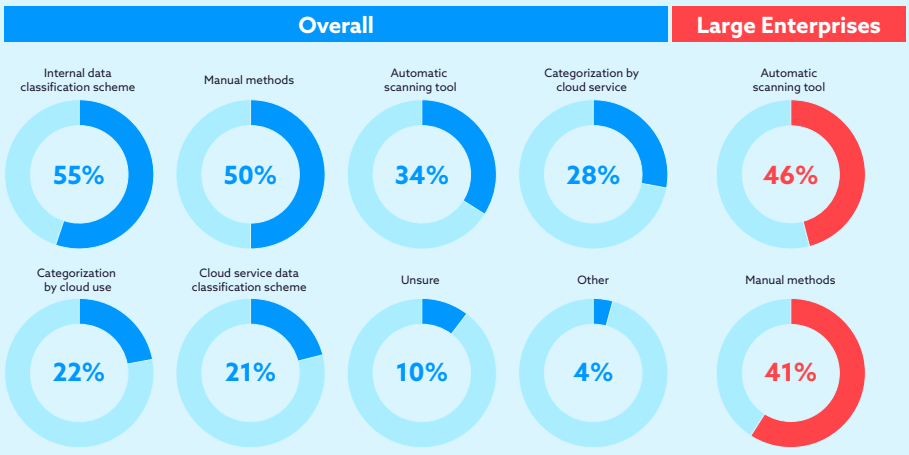
With a move to improve overall business risk management, the cloud is seen as a shift towards improving an enterprise's risk posture, not just a risk to be managed. In this way, the survey analysis addresses the advancement of cloud without the context of on-premise systems and the maintenance of legacy systems. Evaluating cloud and business risk together gives us a better understanding of the impact IT has on the overall risk maturity across the enterprise. In our evaluation, the improvements necessary to achieve ideal security best practices are different in the cloud compared to on-premise environments.

This study shares a better understanding of public cloud adoption and risk management practices within the enterprise. It also analyzes the challenges of managing and measuring risk in the cloud with some techniques working well and others in need of improvement and replacement. Patterns of stricter risk management processes and altered risk tolerance when using the cloud were uncovered. As in many fields, there is still work to be done as organizations mature their ability to manage cloud and multi-cloud security and risk mitigations. It is observed through this study that these issues are improved in the cloud when compared to current on-premise and legacy IT environments. The analysis shows that while constant improvements are needed, a strategy to reduce risk by IT modernization into the cloud or cloud-like on-premise infrastructure remains an organization›s best path to viable risk management. Risk management practices impact many areas in the enterprise. Modernizing the approach will help both businesses and providers improve the adoption of the cloud. Cloud is becoming less of a risk to manage and more of a means to managing these risks.

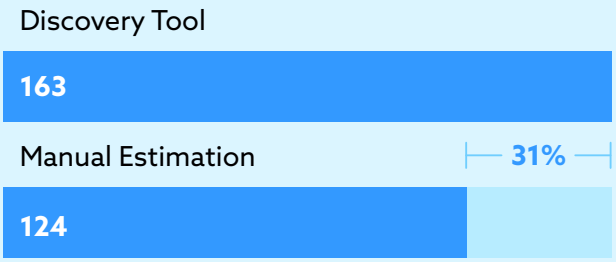
Key Finding 1

As organizations adopt cloud, they are challenged to evaluate risk

Cloud migration presents the potential to unify data collection methods. Yet, internal data classification schemes and manual digital asset management methods are still the primary ways organizations are collecting, tracking, and organizing cloud assets. There is little consistency in how data is classified across cloud platforms and services. Only 21% of users are utilizing native or automated cloud data classification tools and only 65% of those users are aligning with internal data classification schemes. Enterprises interviewed also shared a lack of consistency on how cloud services are being identified and categorized. This lack of data and cloud governance practices adds to the inconsistency in digital asset management.



Modern tools improve asset context and discovery in the Enterprise yet there is a disconnect between what some are observing in their environment. Some of the enterprises interviewed are still evaluating cloud discovery tools. Eighty-five percent of the number of cloud services reported from the survey were using manual approximation methods. The average manual approximation of cloud services (124) is 31% below the average reported with a discovery tool (163). Other sources1 have shown this to be even more inflated. Ultimately, governance models must mature to include automated tools and processes for more effective management of digital assets.



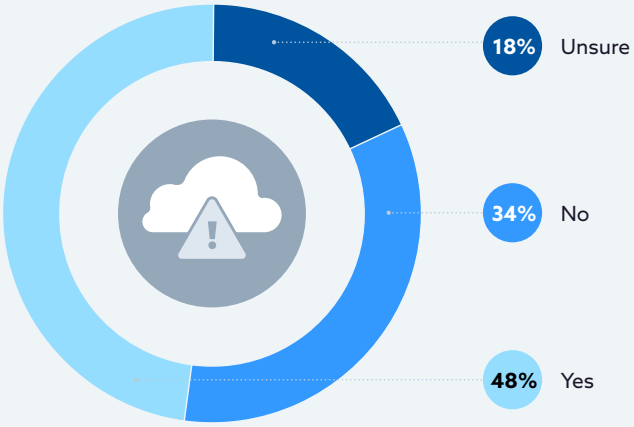
The inconsistent reports of shadow IT also show a lack of standard categorization and governance in the cloud. Enterprises interviewed intend on increasing their workloads in the cloud over the next 12 months. With enterprises continuing to add production in the cloud and using more cloud services, managing cloud and digital assets will be critical in the management and measurement of risk in the cloud.

Key Finding 2

Cloud risk evaluation faces challenges with growing business adoption of cloud

The shift to increasing workload production in the cloud and the growth in the use of cloud services is part of modernizing a business and moving towards digital transformation. This is evident with the cloud service usage numbers in addition to the 58% of survey respondent companies primarily using multiple cloud infrastructure as a service (IaaS) providers. With cloud adoption numbers increasing, respondents shared that services are often evaluated at procurement only and not re-evaluated as product features or business environments change. More than half (52%) of organizations reported not evaluating the risk of their cloud services being used after procurement.

Vendor product risk assessments are often done at procurement only while shadow IT services often go unevaluated for risk. Cloud product features change often and dynamic IT environments can cause configurations to shift or drift. These products and services should be evaluated more frequently to keep up with the security risks that they present to the businesses that use them.



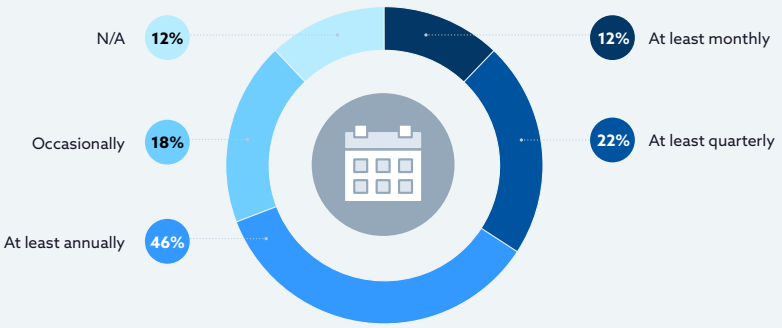
In addition to repeated evaluation of cloud services, the risk management metrics used to evaluate cloud services should be revised. A majority 65% reported adjusting risk metrics annually or less frequently.

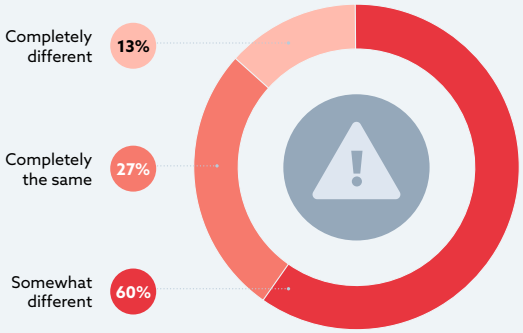
The recent pandemic is an example of an unexpected circumstance impacting the use of third-party solutions. Those with frequent ongoing risk evaluations of vendor products are able to make informed business decisions with services when vulnerabilities and violations are discovered and patched. Others continue to be exposed or lose productivity if they are not able to keep up with cloud risk and business adoption.

1 https://cloudsecurity.mcafee.com/cloud/en-us/forms/white-papers/wp-cloud-adoption-risk-report2019-banner-cloud-mfe.html

https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019

Cloud computing represents a technology shift with a business approach of relying on third parties for operational services and critical business functions. There is still a gap between cloud risk management practices and traditional IT approaches.

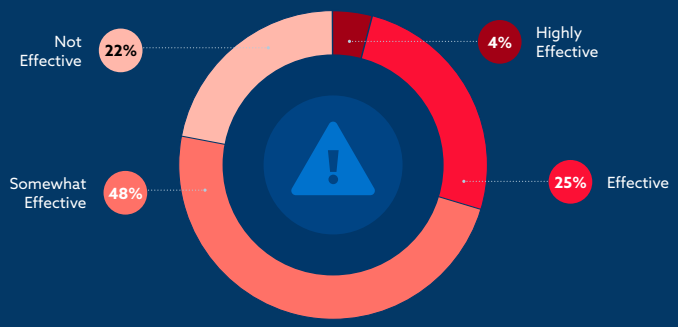




Key Finding 3

Tools for quantifying and measuring risk need to improve

When evaluating effective risk management practices for the cloud, 70% of organizations reported less effective processes for assigning risk to cloud assets. Only 4% reported having highly effective practices. These processes are impacted by the tools and methods used to measure risk for cloud platforms and products



Popular risk scoring tools for quantifying and measuring risk are not meeting expectations but there is a distinction of what tools are working better than others.

	Cloud-Native	Third-Party	Open Source
Highly Effective	4%	5%	15%
Effective	35%	25%	48%
Somewhat	39%	28%	25%
Not Effective	6%	4%	3%

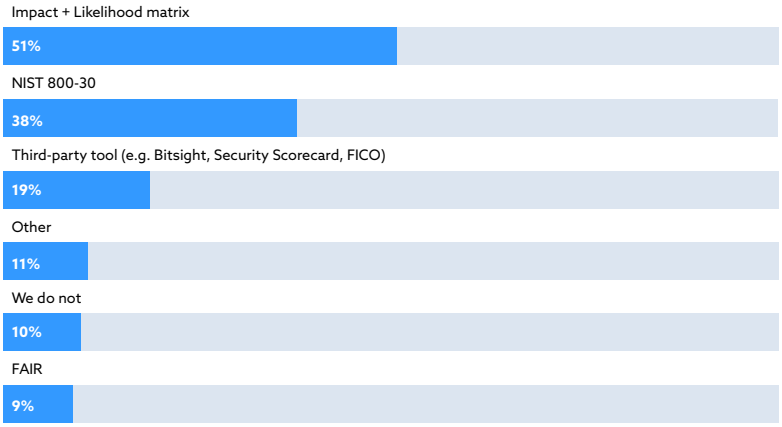
Even though there is room for improving the effective use of risk management tools across the board, open source tools and methodologies lead the way on meeting user satisfaction. Top frameworks used include:

- NIST Cybersecurity Framework (CSF)
- US Department of Defense Cybersecurity Maturity Model Certification (CMMC)
- CSA Cloud Controls Matrix (CCM) and Security, Trust, Assurance, Risk (STAR) Program
- Factor Analysis of Information Risk (FAIR) Institute

Key Finding 4

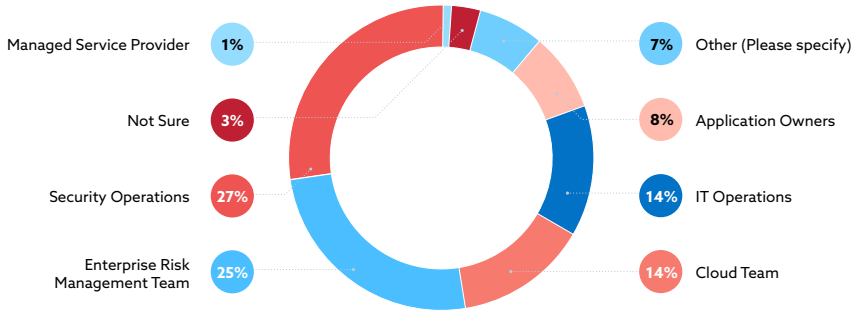
Monitoring, measuring, and reporting risk is difficult

There are a vast number of tools used to monitor, measure, and report risk in the cloud. The metrics for measuring risk provided by each tool do not always disclose whether measurements reflect risks that are cloud-native, third party, or open source . The exception is open source frameworks and tools that share a defined set of criteria which may be why open source tooling was reported as more effective. Without understanding the metrics behind how risk is measured, 30% of enterprises reported that risk scoring systems are used as a directional guide to risk improvement for certain cloud solutions as opposed to measurements that can be relied on for comparison across all cloud services.



A lack of reliable risk measurement has caused organizations to use more qualitative and less quantitative risk measurement methods. Fifty-one (51%) of organizations reported using the likelihood matrix for cloud risk.

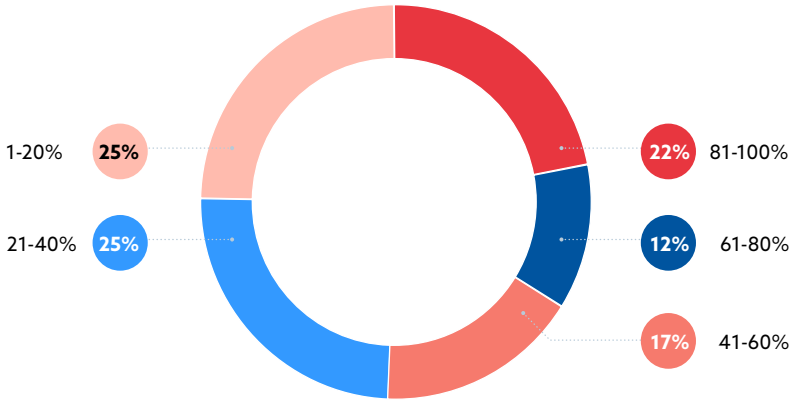
In addition to tools for measuring risk, there are also different teams reported within an organization that monitor and own cloud risk within an organization. The shared responsibility of cloud operations can be unclear and risk ownership seems to add to this complication across the business.



Public Cloud Usage

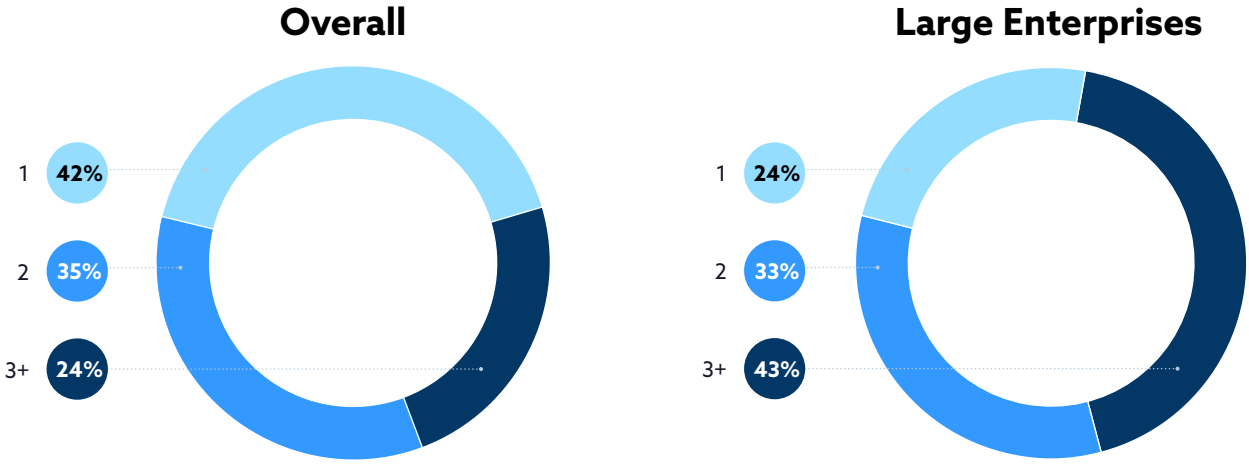
Percentage of production workloads in public cloud

Respondents estimated the percentage of workloads their organization is currently running in a public cloud. Over half (51%) of the respondents run 41% or more of their workloads in the public cloud.



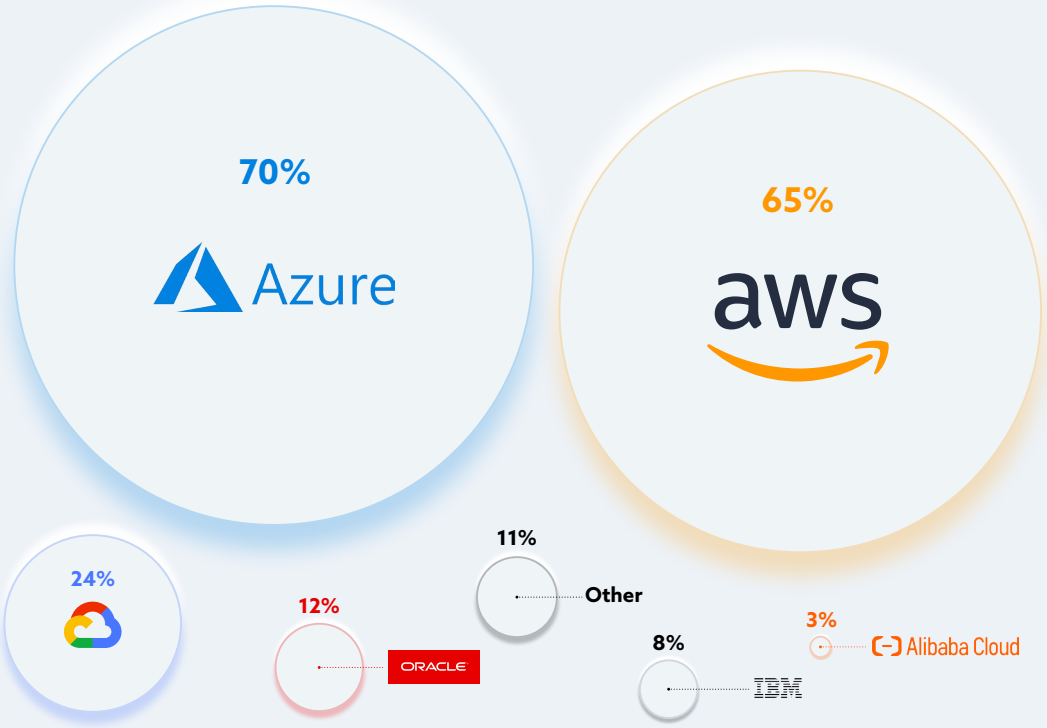
Number of primary IaaS platform(s)

The number of organizations using multiple public clouds strategies has increased. Respondents were asked about the number of IaaS platforms they use. As expected, the majority of respondents use 2 or more IaaS platforms (59%) with 24% using 3+. Large enterprises showed an even greater shift towards multi-cloud environments.



Primary IaaS platform(s)

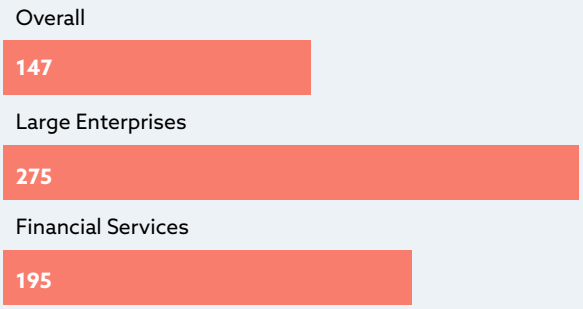
The primary IaaS platform(s) used by respondents unsurprisingly were **AWS (65%)** and **Azure (70%)**. Google Cloud was the third most used platform (24%).

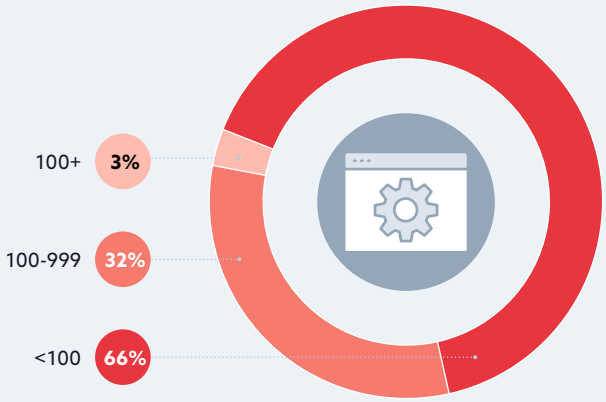


Number of public cloud services used including IaaS, PaaS, and SaaS

Respondents were asked to report the number of public cloud services they use including SaaS, PaaS, and IaaS to better understand organizations› use of public cloud services. In a previous CSA survey in 2020, respondents estimated that they used just 38 public cloud services on average. However, in this survey the average number of services was much higher at 147. To break this down further, 66% of respondents estimate their number of public cloud services to be 100 or fewer, 32% reported a number between 101 and 999, and 3% reported using 1000 or more.

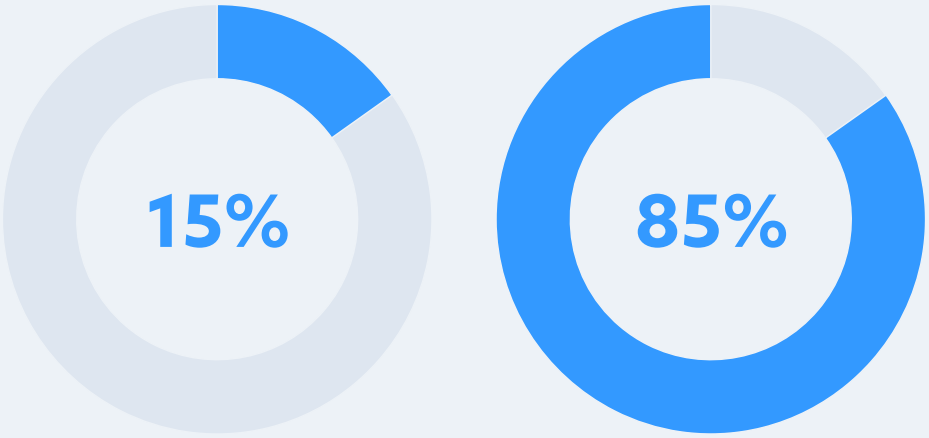
Approximately how many public cloud services does your organization use (including Software as a Service (SaaS) applications)?





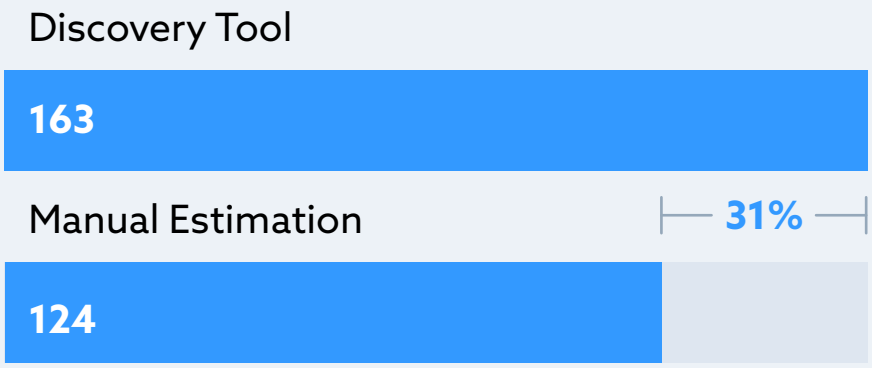
Method for estimating the number of cloud services used

A follow-up question was asked regarding the estimation method used to determine how respondents arrived at the number reported in the previous question . The majority of respondents indicated they were manually approximating (85%). Only 15% were using a discovery tool such as a CASB to more accurately estimate their organization's use of the public cloud.



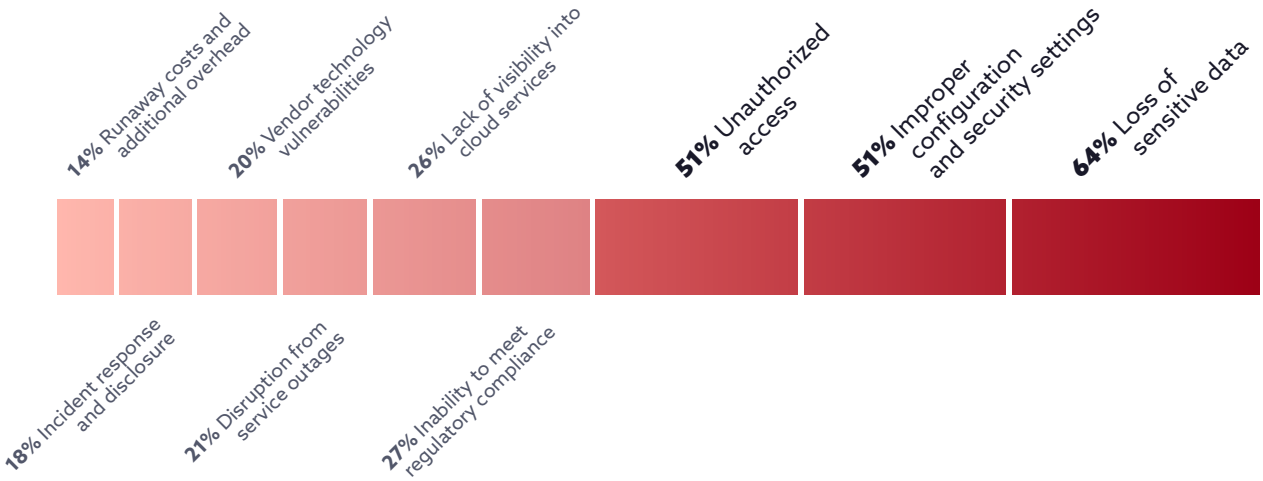
Average number of cloud services: Manual estimation vs discovery tool

The estimated number of cloud services was then parsed by whether the estimation was manual or done with a discovery tool to determine if there were any differences between the two methods. On average, those using a discovery tool reported 31% more cloud services used. This indicates that many organizations have gaps between their actual and estimated use of cloud services.



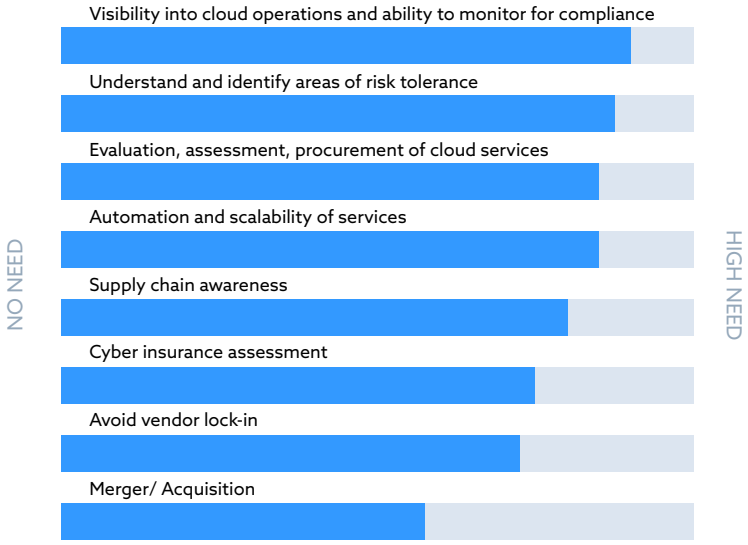
Top security concerns regarding applications running in the public cloud

Respondents were asked to report their top three concerns to better understand the security concerns when running applications in the public cloud . Three concerns rose to the top: loss of sensitive data (64%), improper configuration and security settings (51%), and unauthorized access (51%). The remaining concerns received less than 27%.



Top-rated benefits for managing risk in the cloud

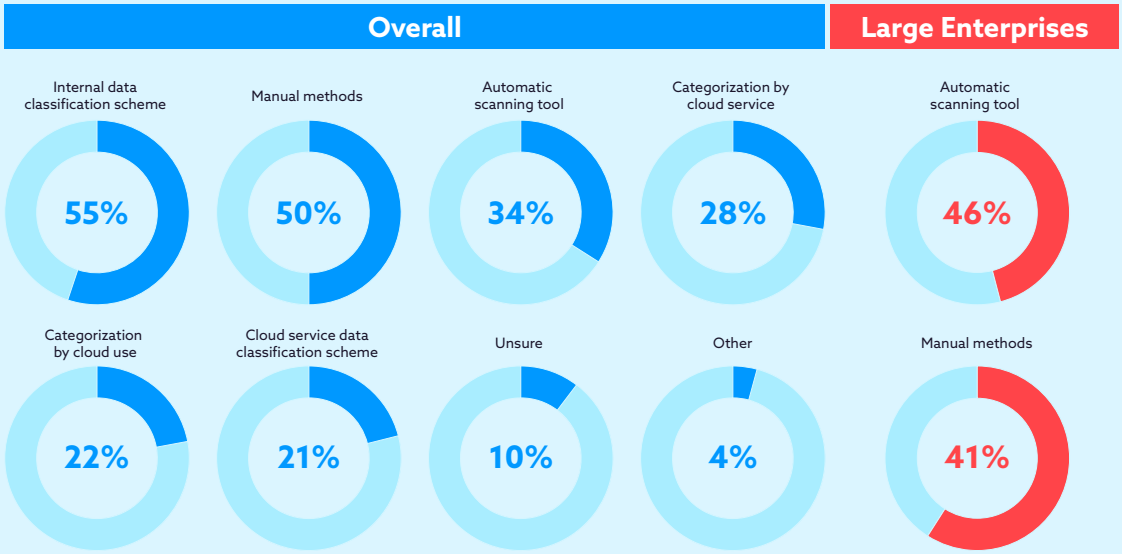
The highest-rated benefit public cloud provided for managing risk was the organization›s ability to track assets and service usage and monitor their configurations for compliance. Coordinated disclosure with cloud services and supply-chain awareness are also notable. The lowest-rated response was mergers and acquisitions.



Cloud Inventory Management

Method for collecting, tracking, and organizing cloud assets

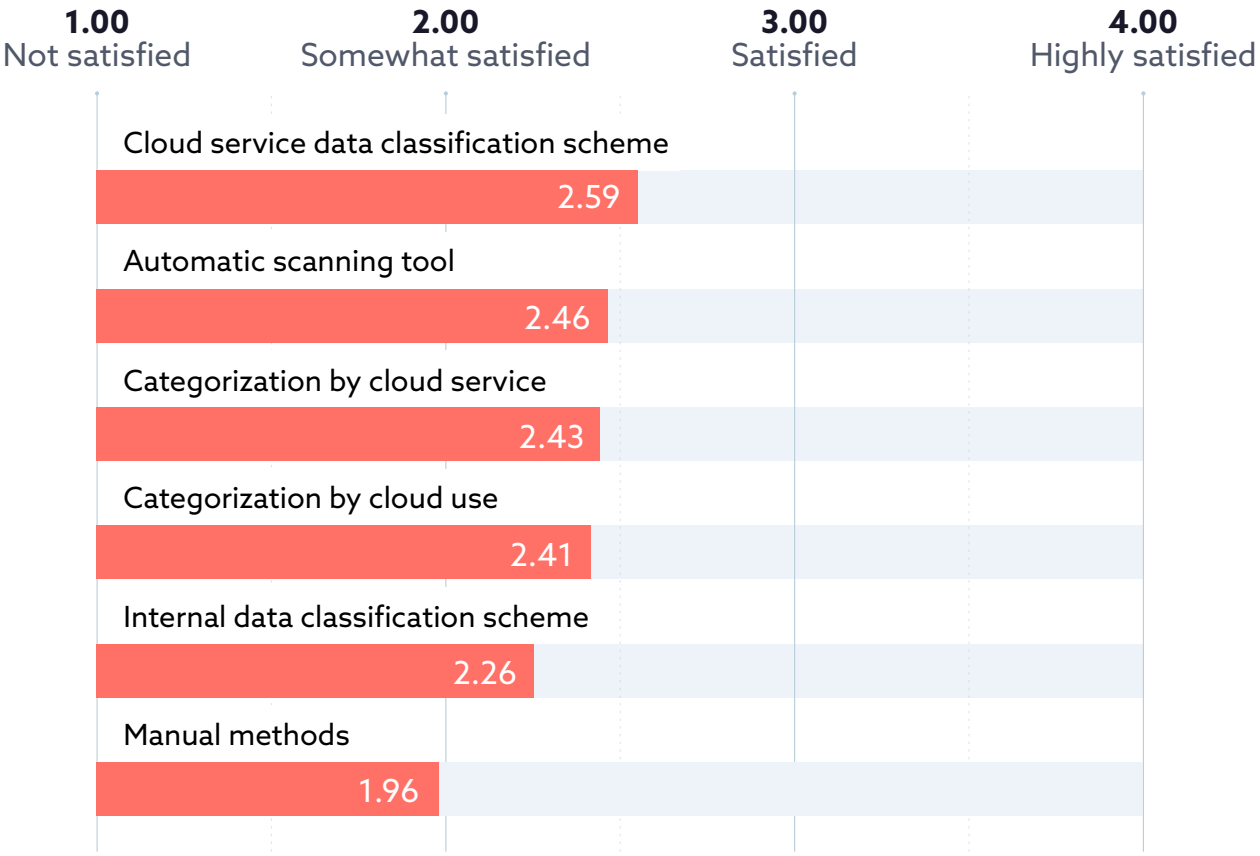
A series of questions about the organization's cloud inventory management practices were asked. Respondents were asked about their organization's method of collecting, tracking, and organizing cloud assets. The most common responses were internal data classification schemes (55%) and manual methods (50%). This indicates that for many organizations standard classification schemes are insufficient or non-existent.



Satisfaction with current methods from collecting, tracking, and organizing for cloud assets

Organizations rated their satisfaction with their current method of collecting, tracking, and organizing assets in the cloud. Overall, respondents reported they were only "somewhat satisfied." When the average satisfaction rating was assessed per method the most common methods "manual methods"and "internal data classification scheme" received the lowest average satisfaction ratings landing on the low end of "somewhat satisfied".

Between the top two methods for collecting, rating, and organizing cloud assets, there was some variation in the average satisfaction rating (Manual method 1.96, Internal data classification scheme 2.26).

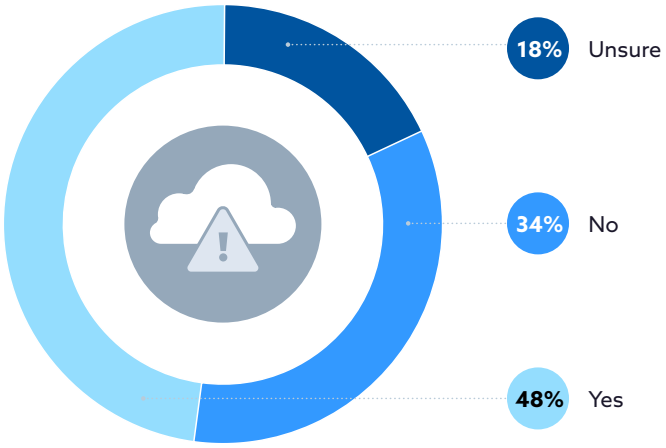


Satisfaction with current method for assigning risk to cloud inventory assets

Respondents were also asked to rate their satisfaction with their organization's method for assigning risk to cloud inventory assets. Again, the average rating was only "somewhat satisfied".

Repeated evaluation of cloud services to adjust risk status

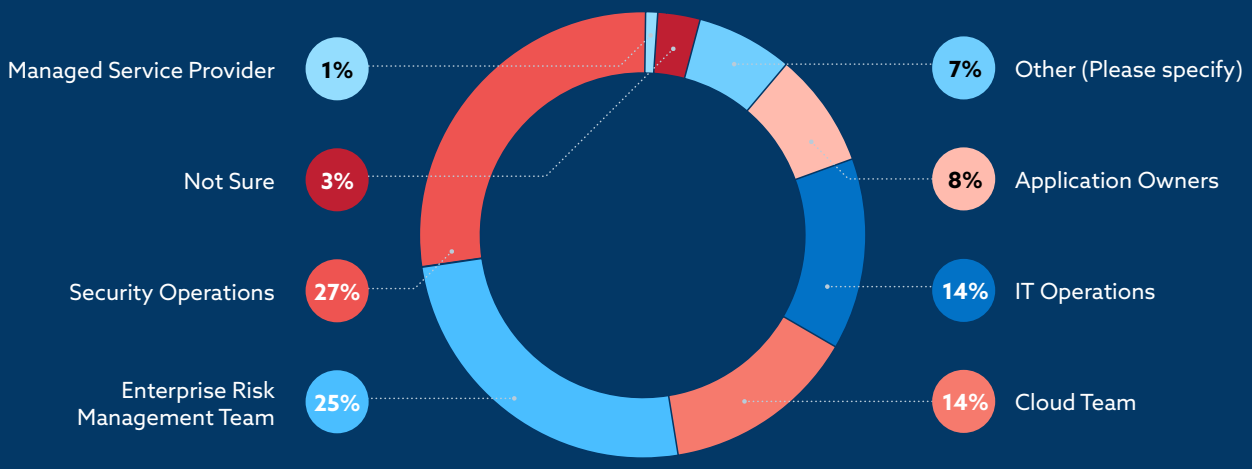
Respondents were asked about whether their organization repeatedly evaluated and adjusted risk status. **48% reported "yes" 34% reported "no."** Since cloud services are ever-evolving and changing, adjusting the risk status is an important exercise to ensure proper security controls are in place. Yet, fewer than half of the organizations repeatedly evaluate cloud service risk.



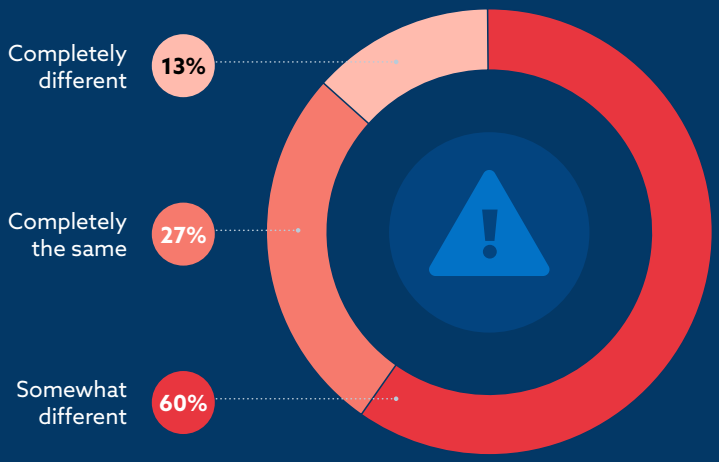
Risk Management Practices

The primary team responsible for managing risk

Respondents were then asked a series of questions regarding their organization's risk management practices. Respondents were asked about the team responsible for managing risk in the cloud. The most common responses were **security operations (27%)** and **enterprise risk management team (25%)**.



The similarity in approach to risk management in the cloud vs traditional IT



Then respondents were asked how similar their approaches to risk management are when comparing cloud and traditional IT. **"Somewhat different"** was the most common response (60%). Twenty-seven percent reported that they were **"completely the same"** which left only 13% as **"completely different."**

Satisfaction with third-party vendors for managing risk in public cloud

Respondents rated their satisfaction with the third-party vendors they use for managing risk in the public cloud. On average for this section, respondents reported they were between "satisfied" and "somewhat satisfied."

Open Source Standards/Frameworks used to manage risk in public cloud

Respondents were asked what open-source standards or frameworks they use for managing risk in the public cloud for their organization. The most common framework was the NIST Cybersecurity Framework (72%) followed by CSA's CCM/CAIQ (41%), leaving only 7% using the Department of Defense Risk Management Framework.

Satisfaction with open source standards/ frameworks for managing risk in public cloud

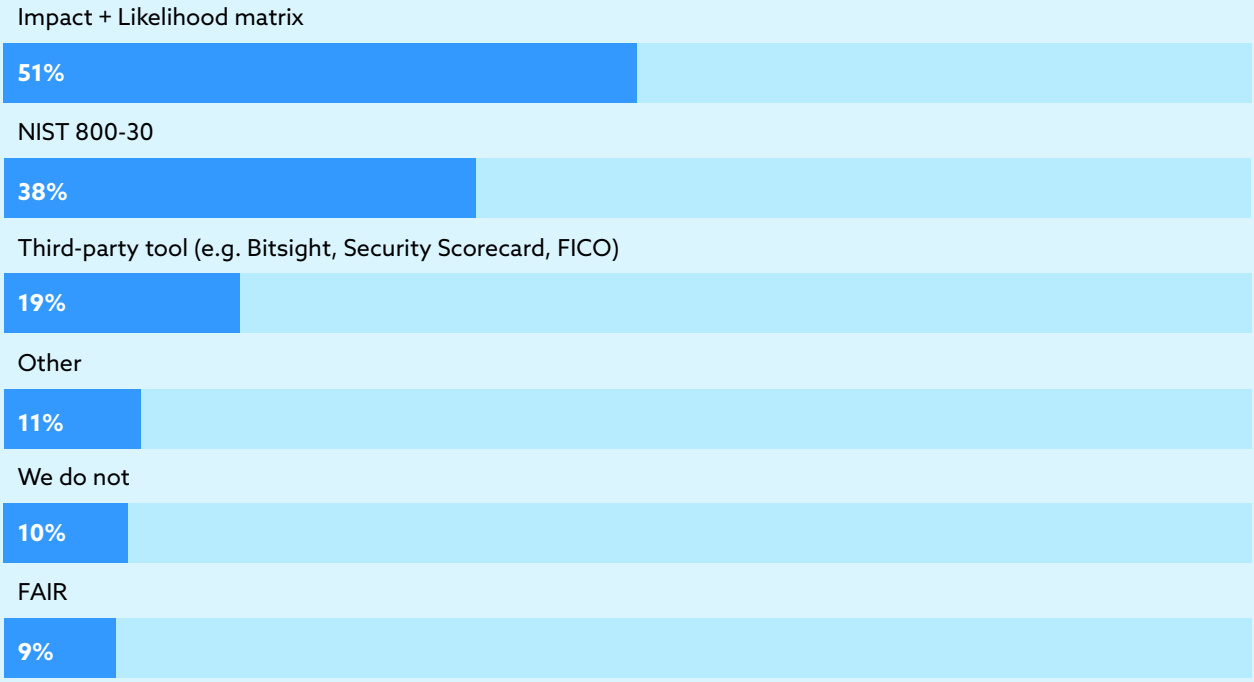
Respondents rated their satisfaction with these standards and frameworks as "satisfied" which is the highest average rating of any of the methods and tools used to manage risk in the public cloud.

When comparing the satisfaction rating for NIST CSF, CCM/CAIQ, and DoD, there were no significant differences in the average rating (NIST CSF = 2.9, CCM/CAIQ = 2.9, DoD = 3.0 or Effective)

Quantifying Risk

Method for quantifying or calculating risk

A series of questions were asked regarding their methods and satisfaction with quantifying risk to better understand how organizations are calculating risk. Organizations indicated "Impact + Likelihood matrix" followed by "NIST 800-30" (38%). Interestingly 10% of respondents reported that their organization did not quantify risk.

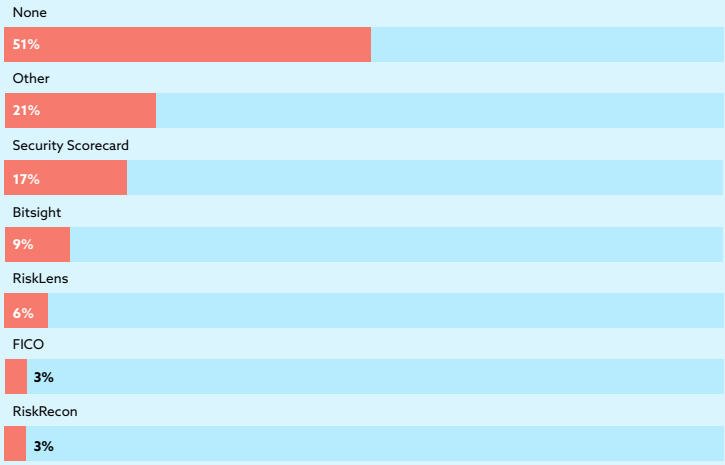


Effectiveness of current method for quantifying or calculating risk

Overall satisfaction with organizations' current method for quantifying risk averaged around "somewhat satisfied," when rated on a scale from 1 - Not satisfied to 4 - Highly satisfied. No significant differences were found between the options. NIST 800-53, third-party tools, and FAIR all received a 2.7 average rating. Impact likelihood matrix received a slightly lower rating 2.5 - interesting since it's the most popular.

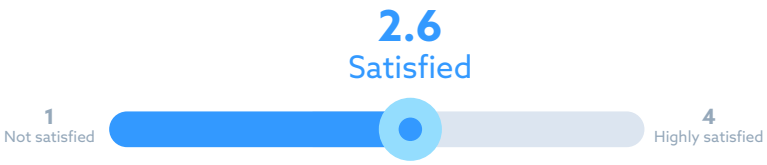
Vendors or tools used to quantify or calculate risk

When asked about the vendors or tools used to quantify risk, the most common response was "None" (51%). There was a relatively even spread of organizations utilizing vendors.



Rate your satisfaction with the tools/vendors you use to measure risk.

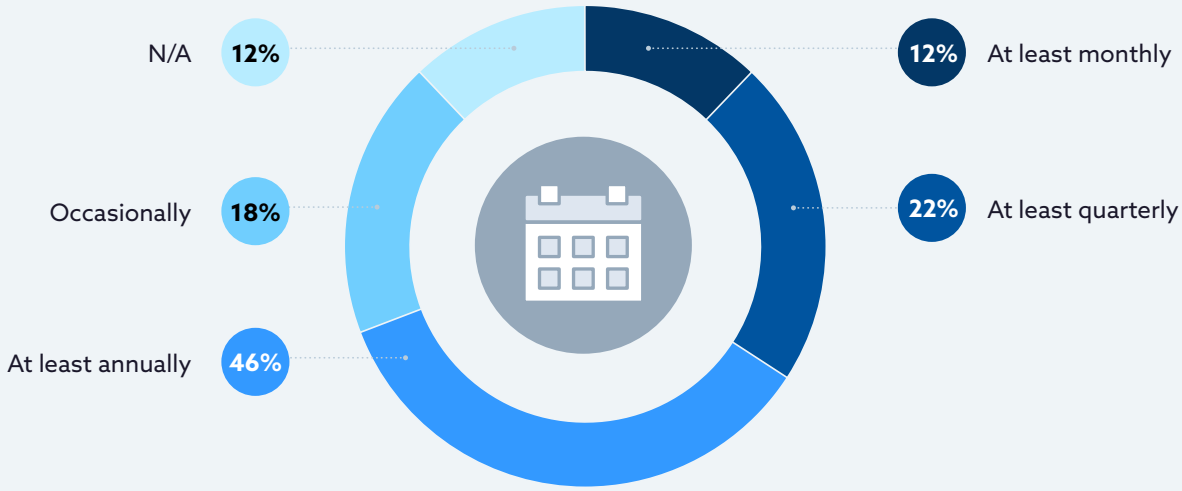
Of those who provided a response on the previous question other than "none", on average, they rated their satisfaction with the vendor for measuring risk as "satisfied."



Risk Management Impact

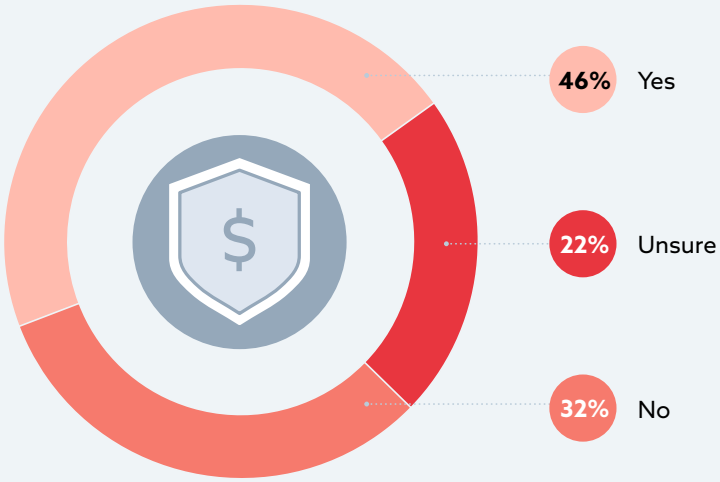
Frequency of revisions for risk management metrics

Respondents were asked how often they revised their risk management metrics. The most common response was "at least annually" (35%) followed by "at least quarterly" (22%).



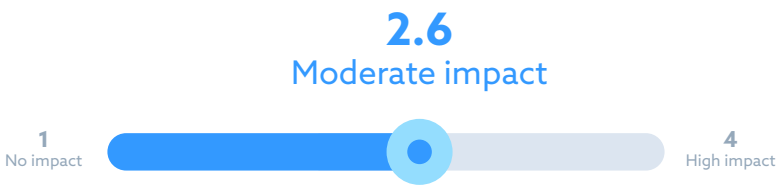
Cybersecurity insurance coverage

Respondents were then asked whether or not they had cyber insurance coverage. Just under half (46%) reported that they did have cyber insurance. Under a third (32%) reported not having cyber insurance and under a quarter (22%) reported they were unsure.



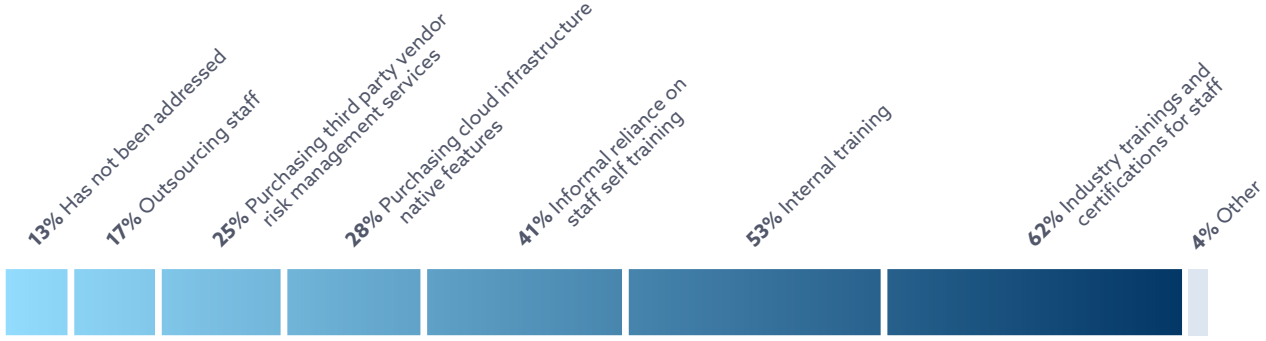
Level of impact risk management approach has on cybersecurity insurance coverage

Those who reported having cyber insurance in the previous question were asked a follow-up question regarding the level of impact their organization's risk management approach has on their cyber insurance coverage. On average, respondents reported it had a "moderate impact."



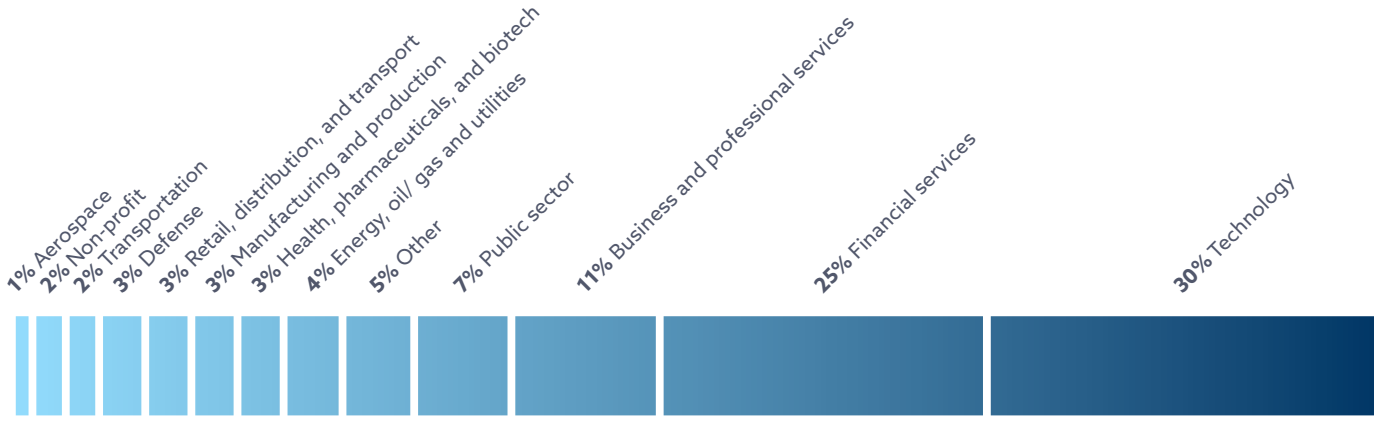
Methods for keeping up with current risk management practices in the cloud

Finally, respondents were asked what methods they used for keeping up with current risk management practices for cloud. The most common responses were as follows: industry training and certifications for staff (62%), internal training (53%), and informal reliance on staff self-training (41%).

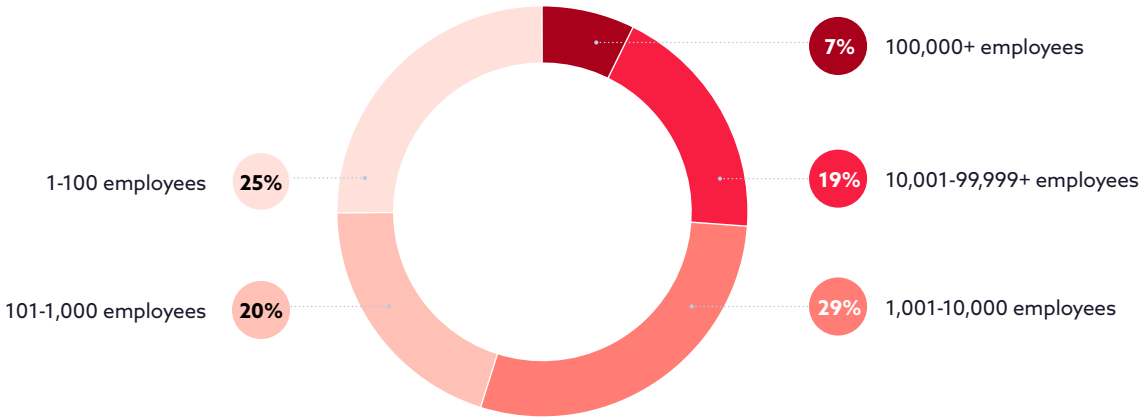


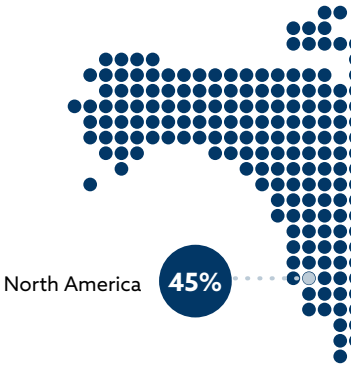
Demographics

Industry

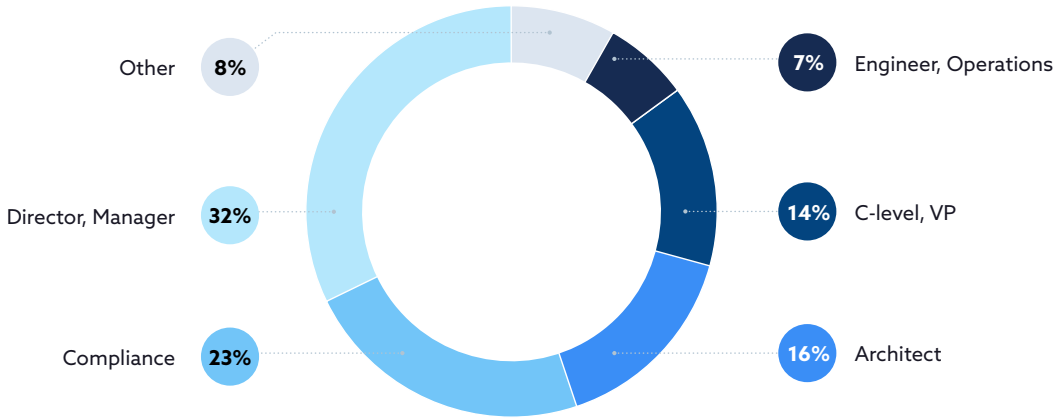


Organization Size

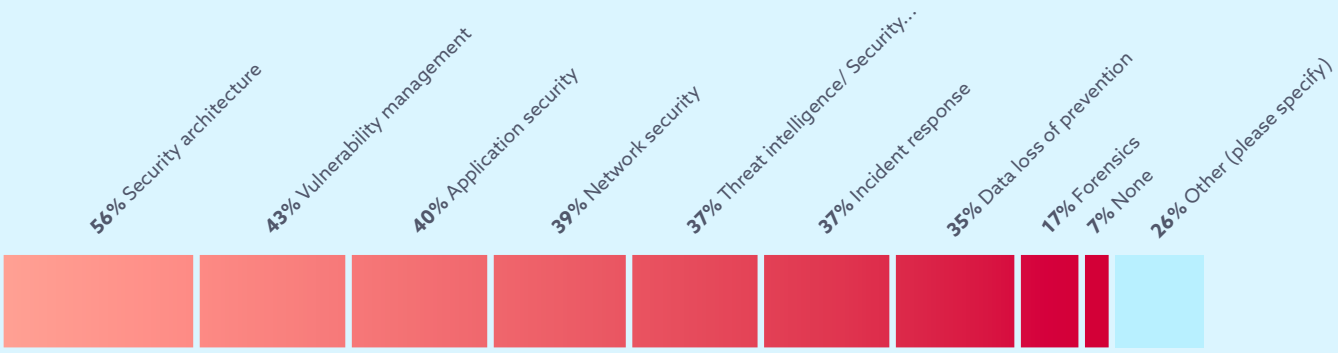




Primary Role



Role in Security



Organization Location