Cloud Usage in the Financial Services Sector

Banking on the Cloud: Real-World Use, Challenges and Opportunities across the Banking and Finance Sectors

cloud security alliance®

Thank You to Our Sponsor

The Cloud Security Alliance (CSA) is a not-for-profit, member-driven 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, certification, events and products. CSA's activities, knowledge, and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. CSA research prides itself on vendor neutrality, agility and integrity of results.

Thank you to our sponsor, McAfee, for helping fund the development of the research and ensuring quality control through the CSA research lifecycle.

Sponsors are CSA Corporate Members who support the findings of the research project but have no added influence on the content development or editing rights of CSA research.

Acknowledgements

Lead Authors:

Craig Balding
Brian D. Becker
Brandon Galbraith
Jim de Haas
Bill Izzo
Micheal Kroupa
Denny Prvu
Damir Savanovic
John Yeoh

Special Thanks:

The CSA Financial Services Working Group

Table of Contents

Introduction

This survey was created and completed by members of the the Financial Services Stakeholders Platform, a CSA working group whose main objective is to identify and share the challenges, risks and best practices for the development, deployment and management of secure cloud services in the financial services industry. The goal of this survey was to analyze the level of adoption of cloud solutions and requirements from financial institutions' perspectives

In administering the survey, the Cloud Security Alliance's intention was to take the temperature of cloud computing in the financial sector and provide guidance to accelerate adoption of secure cloud services. These takeaways will inform the Financial Services working group and serve as actionable items to address the concerns and opportunities associated with cloud computing and financial services.

This study analyzed the cloud usage of financial institutions across three main areas of interest: security concerns, regulatory requirements, and governance aspects.

The Cloud Security Alliance 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 comprised of 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.

Survey Participant Demographics

Nearly half (46%) are information security personnel; the remaining participants are split between CIOs, CISOs, Compliance Offers, Cloud Operations/Architects, Data Center Architects, DevOps Engineers/Managers and "other."

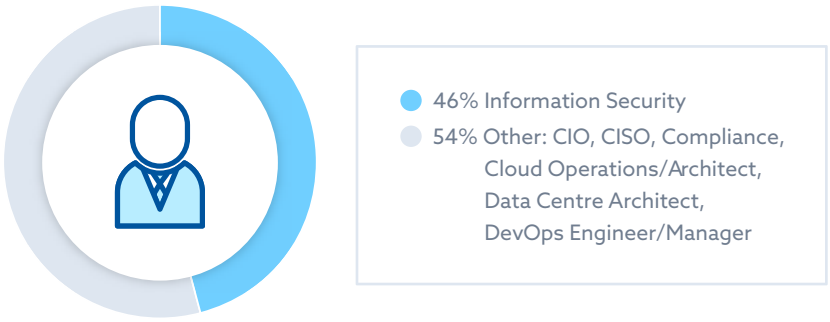

Figure 1 Primary Roles

40% of respondents have over 10,000 employees, 15% between 2000-10000, and 30% fewer than 2000.

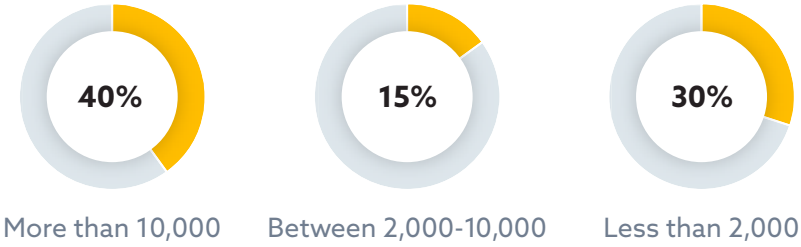

Figure 2 Organization Size

Surveyed organizations have a global footprint, with operations in EMEA accounting for 56%, Americas 37% and APAC 22%.

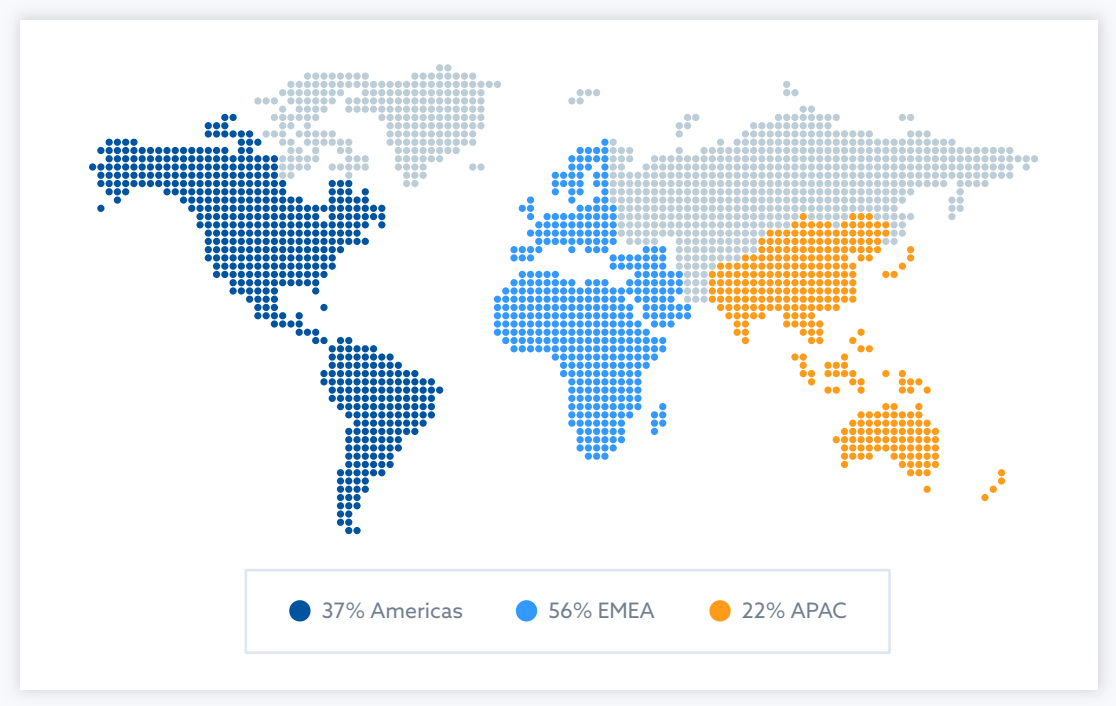

Figure 3 Participant Locations

Nearly two thirds of respondents represent banks and credit unions, 21% insurance, and 12% investment. In addition there are responses from two clearing houses, four professional associations and a Cloud Service Provider.

Current Cloud Use by Participants

91% of respondents are actively using cloud services today or plan to use them in the next 6-9 months. This is double the number since our last survey four years ago. Half of the respondents store or process regulated banking data in cloud services already, with a further 10% planning to in the next 12 months and an additional 12% in the next 1-3 years. Slightly over a quarter currently have no plans in this direction.

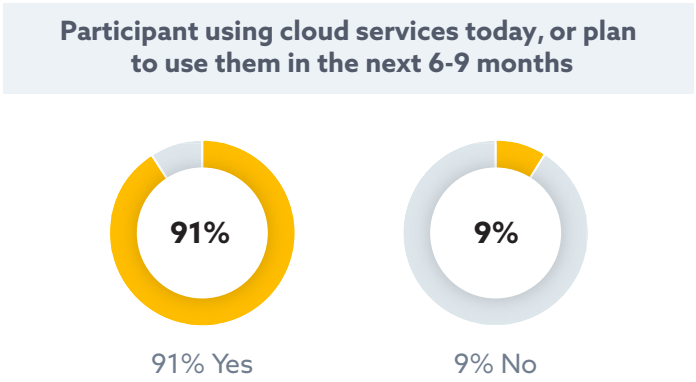

Figure 4 Cloud usage

Cloud for Regulated Workloads

The top quarter of respondents already have over half their regulated workloads in public cloud services, whereas the bottom quarter have none. The middle group is split nearly evenly between those with up to 10% of their regulated workloads hosted in public cloud services and those with up to half of their workloads publicly deployed. Regulated workloads are defined as those that a relevant regulatory authority would consider regulated.

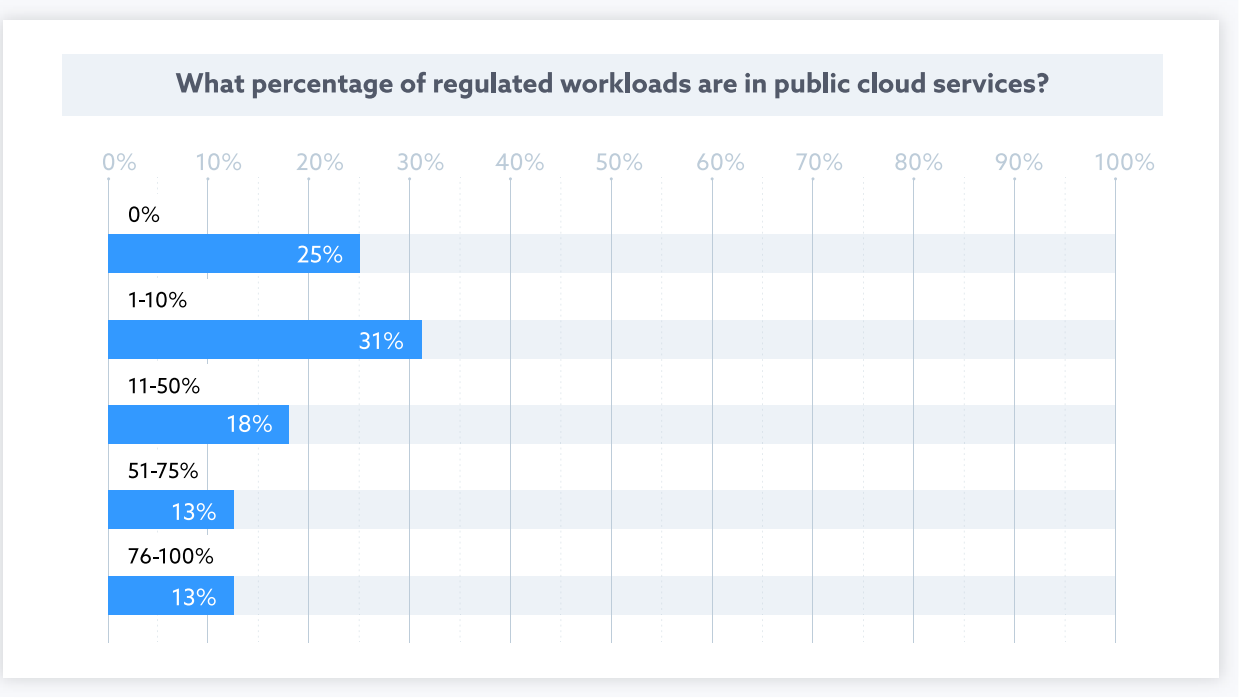

Figure 5 Regulated data

Business Critical Workloads

13% of respondents have 3/4 or more of their organizations' "business critical" workloads or services hosted in production at cloud providers, whereas 17% have none. The majority (46%) have 1-10%.

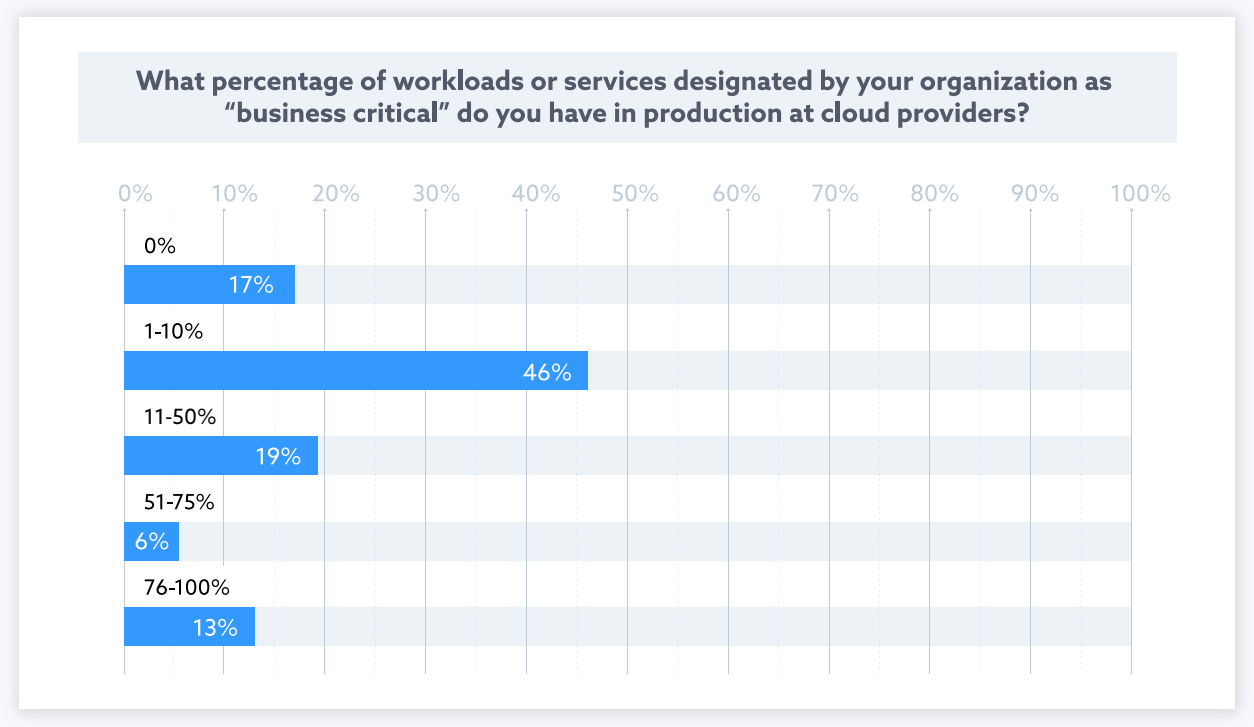

Figure 6 Regulated data

Confidential and Highly Sensitive Workloads

Nearly one fifth of workloads that respondents classify as "highly sensitive/restricted data" operate in public cloud services today. The same is true for one third of workloads classified as "unlimited confidential" (bulk confidential data) and 65% of "constrained confidential" (this means types of information the respondent considers confidential but is limited in data quantity/volume or sensitivity due to internal concerns, rather than technical constraints). Finally, four fifths of respondents' "public domain" workloads operate in public cloud services.

Key Cloud Concerns & Challenges

What are the adoption blockers?

Respondents' concerns are spread nearly evenly across the following key areas:

- technical cyber/security control gaps;
- assurance concerns with cloud provider/service;
- meeting regulatory compliance;
- data privacy rules;
- contractual issues with cloud providers related to risk/security/liability;
- unmet requirements from internal compliance functions.

Since the results reveal no single dominant blocker, the survey analyzes specific concerns and challenges facing banks and financial services across technical controls, risk management, threat monitoring, cloud sourcing and backout plans.

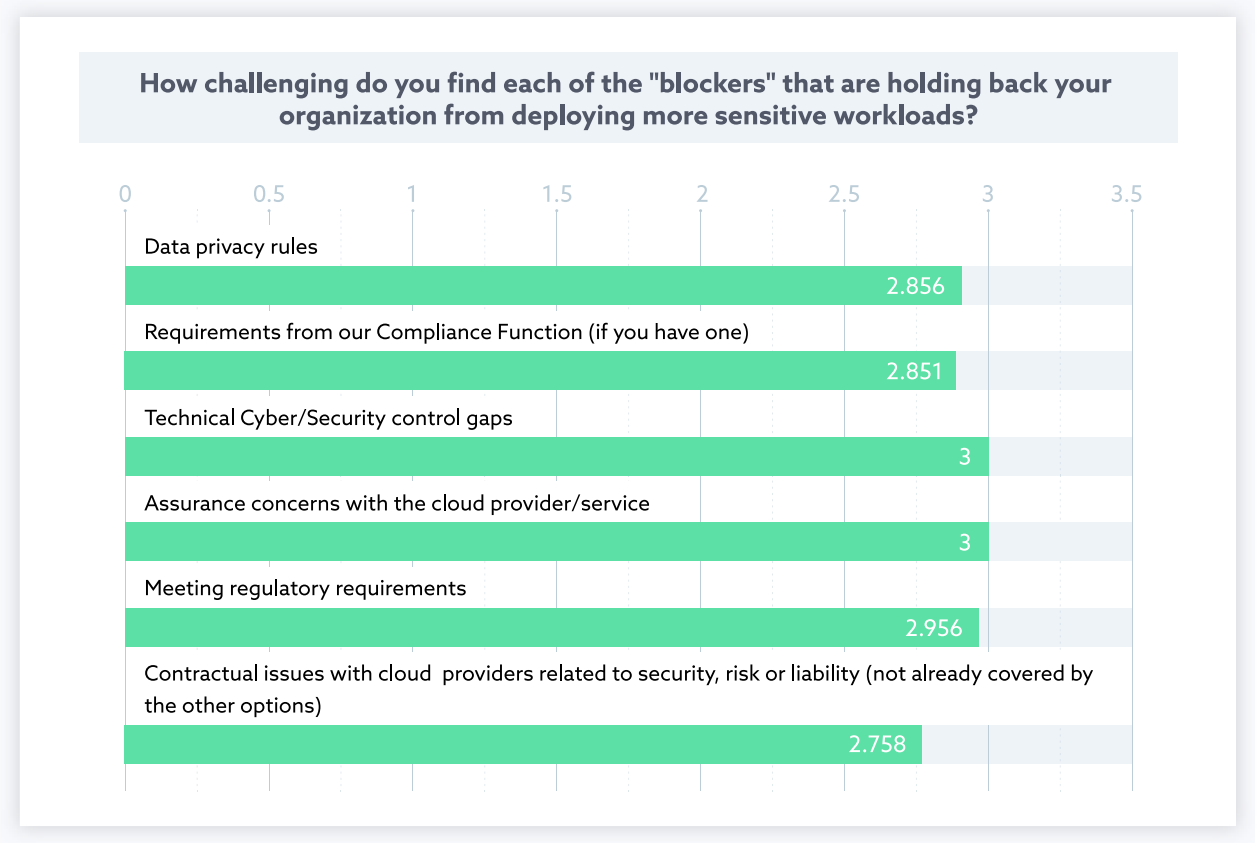

Figure 7 Blockers

Technical Controls: Key Management

Key management for cloud workloads is often raised as a cloud security challenge. Respondents were asked what their organizations' policy position is on key management for different classes of data, and in particular, who "holds the keys"?

Around 90% of respondents have a defined key management policy applicable to regulated and critical data. 42% require on-premise key management for regulated data and 49% for critical data. For all data sensitivity types, Cloud HSM - where master keys are stored in a cloud-hosted HSM (hardware security module) and where the CSP cannot access key material - is strongly preferred over BYOK: 3 to 1 for both non-sensitive data and critical data and 2 to 1 for public and regulated data. Nearly half (47%) of respondents are subject to key management obligations agreed to or accepted with third parties (e.g. regulators, clients, suppliers) for non-sensitive and public information.

CSA corporate members within the FSSP have noted that many SaaS providers do not offer a BYOK feature. This has slowed adoption or limited use cases to better understand the benefits and challenges. There are leaders in this space, such as, Keysafe by Box. Other approaches include Hashicorp's Vault product which multiple member banks are either exploring or using. Based on the report findings, the market needs to develop in this area.

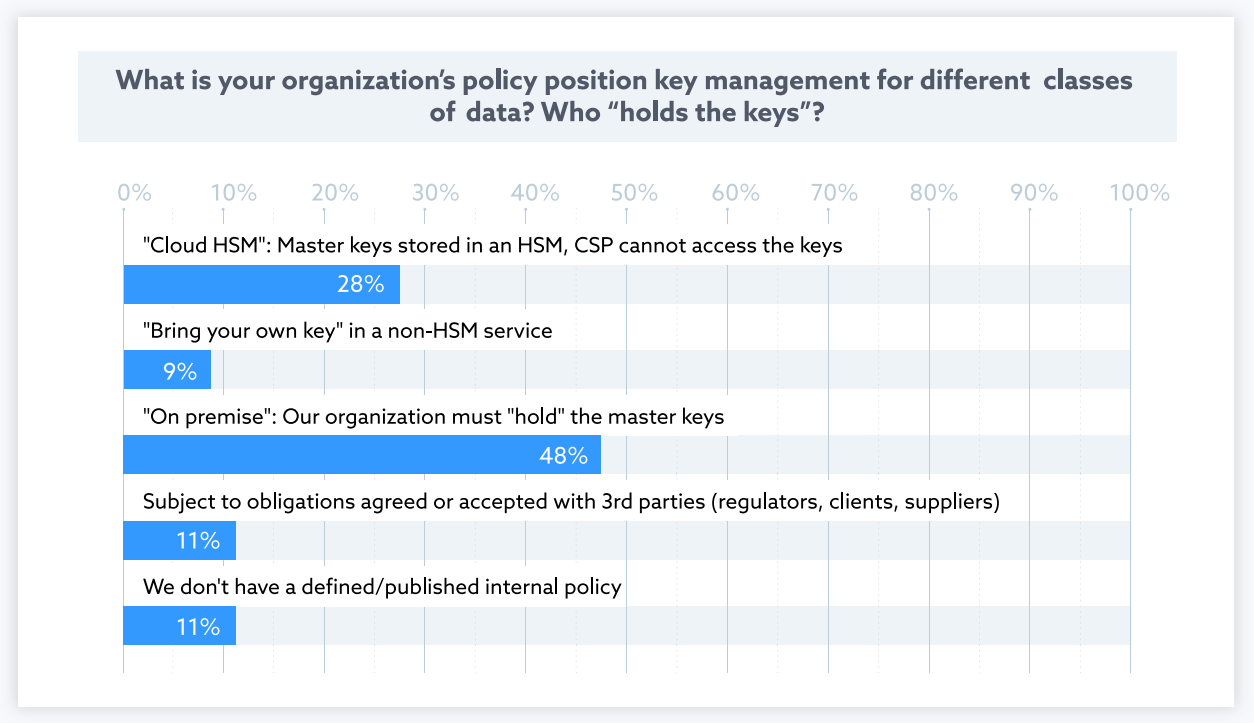

Figure 8 Key management

Reference: Interested readers should consider joining CSA Key Management Working Group: https://cloudsecurityalliance.org/research/working-groups/cloud-key-management/

Risk Management: Policy, Assessment & Talent Risk

Policy: Over half (52%) of respondents have a formal cloud security policy or standard as part of their overall Enterprise Risk Management Framework (ERMF). One third are in the process of developing one and 14% of respondents do not have one.

Risk Assessment: Just over half (52%) of respondents have fully integrated their cloud service risk assessments into their overall company risk assessment methodology. 40% have partially integrated and the remainder have not.

Talent Risk: Only one respondent claimed they have no cloud security skill gap within their organization. For everyone else, the most popular approach to addressing the cloud security skill gap is by developing existing staff (75%). Third parties are used 58% of the time along with hiring external cloud security professionals (40%). Finally, technology and automation are used by about one third of respondents (37%).

CSA financial members are looking for guidance tools and skills to develop cloud security policies that meet industry standards for security. Assessments tools, like CSA STAR[1], outlining security criteria for cloud are being integrated into company risk methodologies but the report findings support other sources[2] that indicate a shortage on skills for cloud security and risk management across the industry. CSA will further develop training[3] for employees and industry professionals on cloud security, auditing, and risk management. The collecting and cataloguing of sample used cloud policies and templates will also be explored.

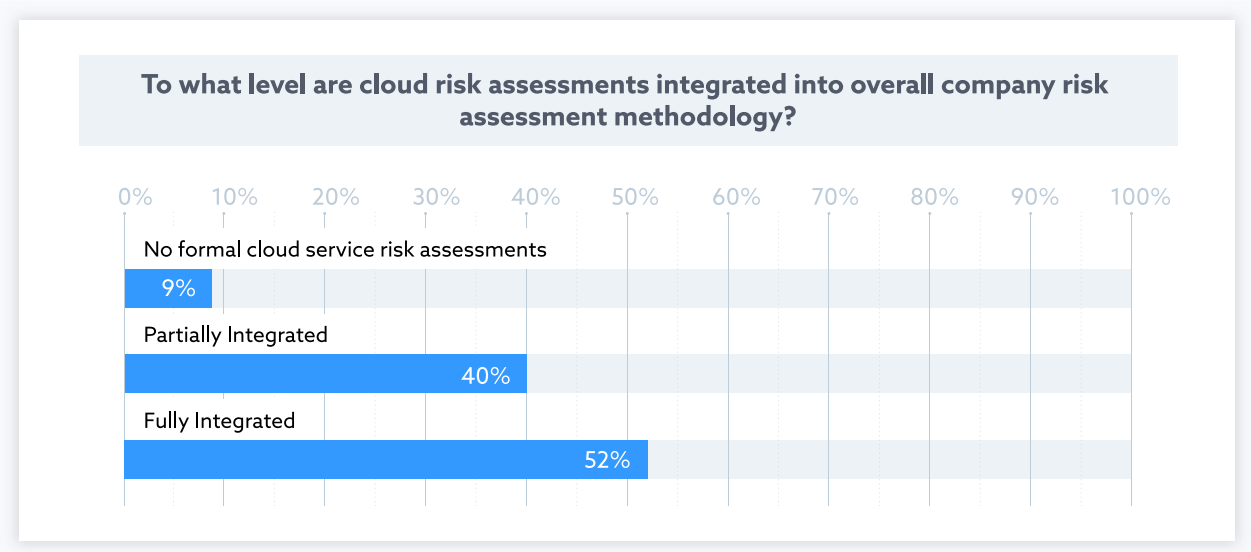

Figure 9 Risk assessments

[1] https://cloudsecurityalliance.org/star/
[2] https://cybersecurityventures.com/jobs/
[3] https://cloudsecurityalliance.org/education/

Threat Monitoring

Respondents were asked to rate their threat monitoring capability (i.e. visibility) for different cloud delivery models.

Organizations consistently rated their threat monitoring capability ("visibility") of cloud services as strongest with IaaS. 21% of respondents consider they have excellent visibility, 47% good and 21% reasonable. Few respondents (7%) consider they have excellent visibility of PaaS and SaaS services. About 36% rate their visibility of SaaS as "reasonable, with some improvement needed" with 12% having no - or minimal - visibility. The PaaS visibility numbers fall in between IaaS and SaaS.

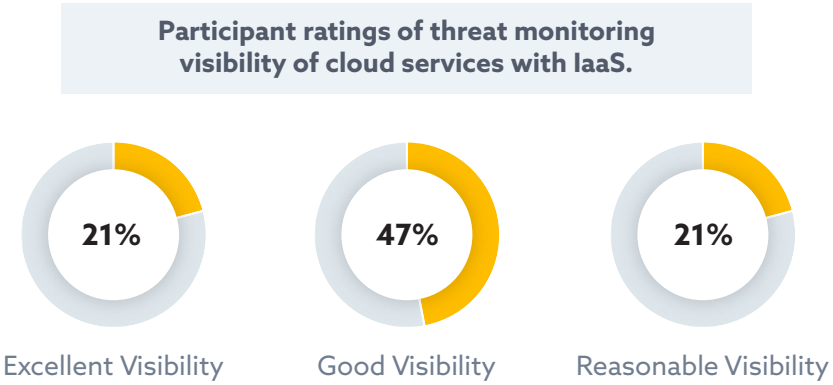

Figure 10 Threat Monitoring

The prior CSA financial services survey[4] indicated the top desired feature by 80% of the survey respondents for cloud services was "increased transparency and better auditing controls". The current report finding suggests that cloud security transparency has improved with the high visibility rating across the cloud deployment models. CSPs offer more tools and better dashboards including integration possibilities with third-party monitoring tools. However, integration and visibility with SaaS falls below the other deployment options. With SaaS services reaching over $100B in revenue last year (2019[5]) and the continued growth of 20% expected in each of the coming years, SaaS governance is in area that will need more focus by CSA researchers and the user community.

Cloud Sourcing

Two thirds of respondents are approved to use multiple cloud providers, with the other third dependent on a single cloud provider. Obvious reasons to use multiple cloud providers is to avoid vendor lock-in and the reliance of one service provider. However, CSA members also suggest the ability to use the best features and functionality of each cloud infrastructure or platform for a specific purpose as a reason to use multiple IaaS and PaaS providers. Internal teams also have a preference toward specific tools offered by each provider in use. Additionally, some cloud IaaS and PaaS providers offer more compliance support than others in the highly regulated financial services industry.

[4] https://cloudsecurityalliance.org/artifacts/cloud-adoption-in-the-financial-services-sector-survey/
[5] https://www.srgresearch.com/articles/saas-spending-hits-100-billion-annual-run-rate-microsoft-extends-its-leadership

The motivation towards multiple IaaS and PaaS providers brings the need for improved multi-cloud orchestration tooling and dashboards as emerging gaps for CSA members.

Backout Plans

Nearly two thirds (63%) of respondents have a manual backout plan in place to change cloud providers, with nearly half having tested the plan. Just over a third have no backup plan to change cloud providers.

Over a third (37%) of respondents have introduced automation to their backout process, with 17% primarily automated, 15% fully automated, and 5% regularly switching their workloads between cloud providers in a "business as usual" way. It has been noted by CSA members that the cost to move data between cloud services can be significant. The reverse flow of data from a specific cloud service far exceeds the movement of data to the cloud for backup.

Recommendations

Based on the survey results, key recommendations are that cloud consumers should continue to pressure cloud providers in two key ways:

- Addressing institutions' technical security requirements and controls needs during procurement and contract negotiations
- Driving increased assurance through continuous demonstration of compliance via third-party audits as opposed to periodic demonstration of compliance.

Enterprises should drive Cloud Service Providers to the same level of rigor in relation to demonstration of compliance as on-premise services and service providers. Organizations have varying maturity levels for consuming and presenting this information and have found three common levels that can be applied.

The first foundational step is to ensure due diligence with Cloud Service Providers in accordance with the manual processes for scheduled follow up and documentation with an archive of activity. The following steps involve slowly moving the manual processes to regular ingestion of compliance information with a goal of an automated dashboard and ingestion process to show continued compliance. All Cloud Service Providers are not at the same level of maturity for not only continuous compliance, but real-time representation of compliance; however, enterprises should leverage technology that is available and drive the service providers to this increased security posture.

There are concerns about concentration and aggregation risk. The European Banking Authority (EBA) prescribed that Outsourcing Function shall report this to senior management. Only regulators have a joined view of an institution's use of specific cloud providers and services for regulated workloads. Financial institutions and other enterprises within CSA should investigate research to investigate alternative solutions to protect data when the encryption offered by Cloud Service Providers does not satisfy security policies. Data classification and Data Leakage Prevention paired with a CASB solution that can hook into SaaS environments can mitigate some of the risk.

Conclusion

The world of IT banking has changed considerably in the past four years in terms of the adoption and usage of cloud computing technology. The finance industry has moved from "dipping their toe" in the cloud, through experiments and proof of concepts, to material and structural use cases supporting key products and services.

A shift in the concerns of financial institutions is visible. Respondents have moved from technical issues to regulatory and contractual concerns. Themes like education and skill set have come to the fore (perhaps in part driven by adoption of agile practices as exemplified by DevOps).

Cloud technology has evolved rapidly in the past years and so has the availability and maturity of cloud security features and controls, for example, the availability of cloud HSM and cloud native security compliance dashboards. For SaaS, bring your own encryption key (BYOK) management issues still exist and present a challenge to adoption. In the area of encryption, respondents indicate there is a deviation from the organization's security policy. The business case for cloud adoption seems stronger than the need for security compliance in the area of key management.

The report demonstrates a fairly high tolerance for financial institutions willing to move regulated data to the cloud based off of business need or competitive advantage. Much remains to be improved upon in the areas of risk, compliance, and security before a preponderance of critical or regulated data is moved to the cloud.

About The Sponsor

As a leading-edge cybersecurity company, McAfee provides advanced security solutions to consumers, small and large businesses, enterprises, and governments. Security technologies from McAfee employ a unique, predictive capability that is powered by McAfee Global Threat Intelligence, which enables home users and businesses to stay one step ahead of the next wave of fileless attacks, viruses, malware, and other online threats. McAfee MVISION cloud-native and insight-driven solutions provide the first cloud-based platform that protects data and stops threats across devices, networks, clouds (IaaS, PaaS, and SaaS), and on-premises environments.

www.mcafee.com