cloud security alliance®

How Cloud is Being Used in the Financial Sector: Survey Report

March 2015

Acknowledgements

Managing Editors / Researchers
John Yeoh
Frank Guanco

Contributors
Mario Maawad Marcos
Willy Leichter
Juan Francisco Losa
Tomas Herranz Medina
Mario Reyes
Maria Luisa Rodriguez
Chenxi Wang

Design/Editing
Texto Graphic Design

Special Thanks
The CSA Financial Services Working Group

Sponsored By

Executive Overview

From research on big data/security to detecting cloud incidents, the Cloud Security Alliance provides a wealth of data and advice on cloud security topics from its expert research and deep bench of information technology authorities. The Financial Services Working Group (FSWG), a new working group within the Cloud Security Alliance (CSA), was created and officially presented at the 2014 CSA EMEA Congress. The FSWG emerged to provide knowledge and guidance on how secure cloud solutions can be delivered and managed by the financial industry.

One of the first actions taken by the FSWG was to build a situation map to show how different cloud solutions are deployed in the financial sector. For this purpose, we offered the survey "How Cloud is Being Used in the Financial Sector" from September through October of 2014. The objective of this study is to understand the needs for adopting secure cloud services in the financial industry by enabling the adoption of best practices. To achieve this, it is first necessary to analyze the financial industry's main concerns regarding delivery and management of cloud services. This encompasses industry needs and requirements, both technical and regulatory, as well as adequate strategic security approaches to ensure protection of business processes and data in the cloud.

In this study, we focused on three areas of interest to analyze the level of adoption of cloud solutions and requirements from financial institutions' perspectives—security concerns, approach to cloud services, and compliance concerns

Several key findings emerged from the study:

- As cloud computing becomes more prevalent throughout the financial sector, a mixed strategy of leveraging both private and public clouds emerge as the norm for most businesses.
- Most organizations do not have a concerted cloud migration strategy.
- Data protection is a preeminent security concern for the financial sector moving to the cloud. In particular, data protection standards and relevant laws are "top of mind" to our survey respondents.
- Industry regulation drives compliance requiring financial institutions to implement specific security measures to consider migrating to cloud services.

In administering the "How Cloud is Being Used in the Financial Sector" survey, the Cloud Security Alliance wanted to take the temperature of cloud computing in the financial sector and provide guidance to accelerate adoption of secure cloud services. The data collected in the survey and the conclusions drawn provides CSA's Financial Services Working Group with an opportunity to refine its goals and deliverables for 2015. These takeaways will inform the working group and serve as actionable items to address the concerns and opportunities associated with cloud computing and financial services.

Table of Contents

Introduction

We circulated the "How Cloud is Being Used in the Financial Sector" survey to IT and security professionals in financial services institutions. The goal was to further the discussion to these topics:

- Describe your company's approach to cloud computing.
- Describe your private cloud policy.
- What is your corporate risk assessment to cloud computing?
- What features would you require from cloud providers?

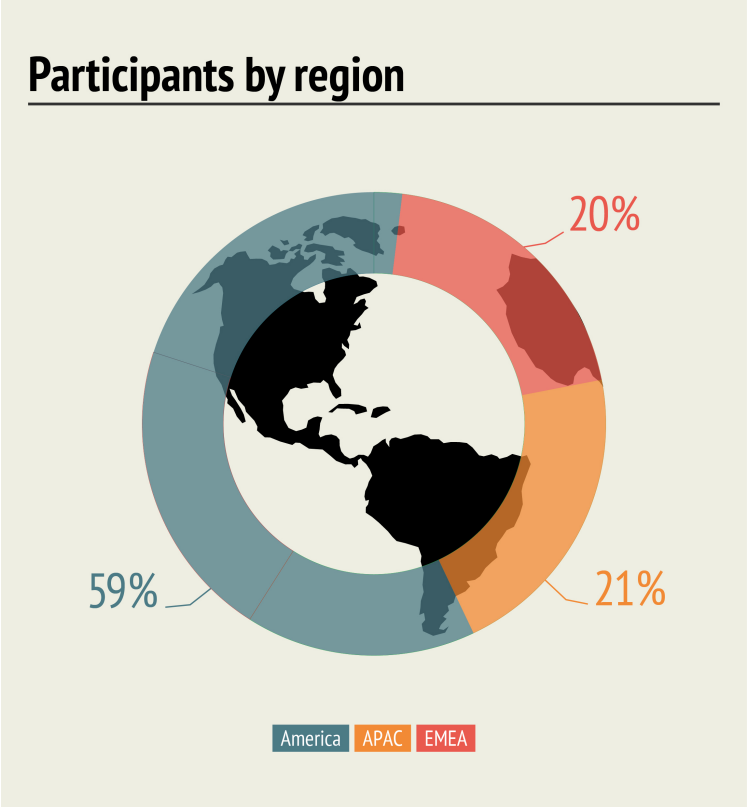
And finally…

What is your primary reason for adopting cloud computing?

Beyond raising awareness around cloud service adoption, the findings of the survey provide insight into how decision makers in the financial services industry take action in their organization – from consolidating and standardizing on the most secure cloud services, to knowing which policies to apply to mitigate risks, and understanding where to focus when educating users.

Survey Participants

The survey attracted 102 participants globally from banking/credit unions (35 percent), insurance (13 percent), investment (11 percent), government (seven percent), and other professional roles (34 percent) over a 13-week period during the fourth quarter of 2014. Participants were spread across 20 different countries, including Americas (59 percent), Asia-Pacific (APAC) (21 percent), and Europe-Middle East-Africa (EMEA) (20 percent) regions. Organizations ranged in size from 1-99 employees (eight percent), 100-500 (12 percent), 501-1000 (three percent), 1001-5000 (16 percent), and 5,001+ employees (59 percent). In terms of the size of the client base of the participants' companies, 26 percent of respondents shared a small client base of between 0-1000 customers, while 32 percent shared a client base of greater than 1,000,000 customers.



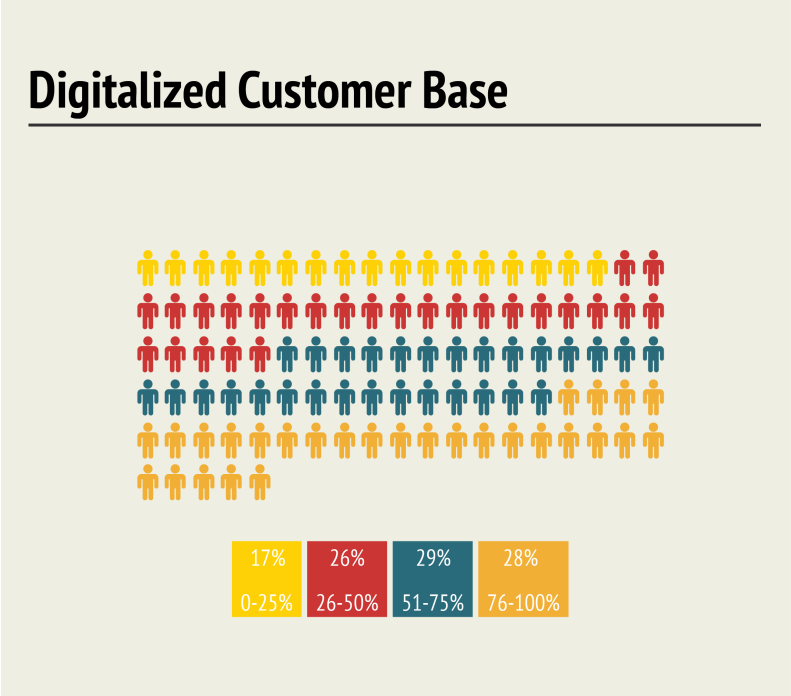
64 percent of the survey respondents were C-level executive or managers in their organizations and the following lists the distribution of their roles.

- Assurance, Security, Audit, or Risk (Information Systems) Management (38%)
- Information Systems Management or IT Professional (34%)
- CSO/CISO (15%)
- Network/Enterprise Architect (7%)
- Line of Business (LOB) owner (2%)
- Other (4%)

Cloud Adoption is Prevalent but Remains Ad Hoc

Customer Influence on Financial Institutions

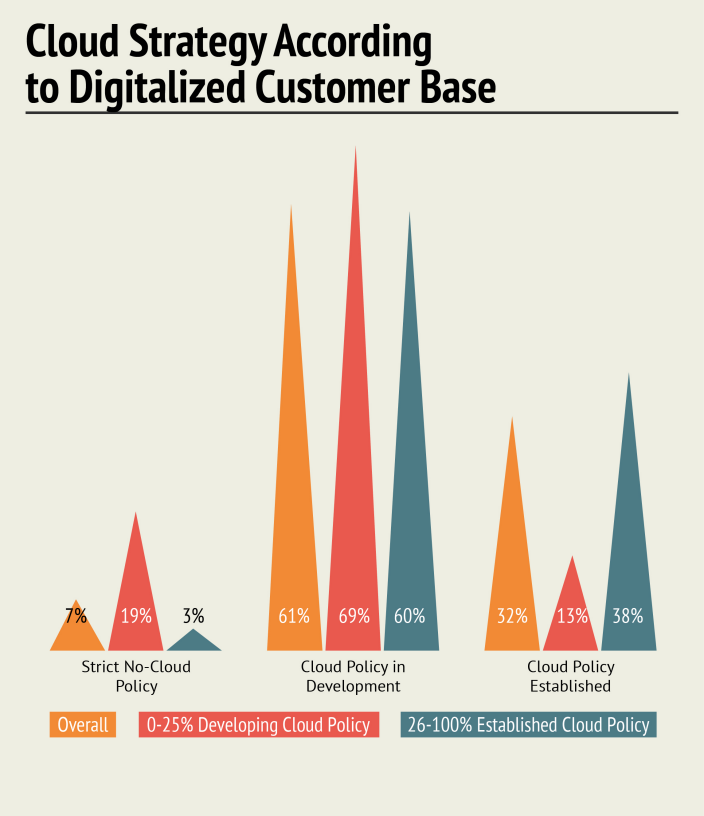
Cloud computing is changing how customers interact with data. This exchange of information between corporations and customers will ultimately impact how the financial industry does business. As we look to better understand cloud adoption in the financial industry, we filtered our survey respondents by region and company size. We also asked those surveyed to share the percentage of their client base that was digitalized. For this study, a digitalized customer is one whose interaction with the bank is at least 50 percent carried out via electronic channels (i.e., online banking, ATM, mobile).



This data provided a context to examine how a financial institution's customer base impacts its approach to cloud computing. Not surprisingly, companies with a small digitalized customer base are more reticent moving to the cloud - 19 percent of companies with less than 25 percent of digitalized customers had a strict no-cloud policy. In contrast, only three percent of companies with 26 percent or higher of digitalized customers had a no-cloud policy. Additionally, companies with existing cloud strategies had a more digitalized customer base at 38 percent while less digitalized customers comprised 13 percent of the companies.

Interestingly, small companies (500 or less employees) and large enterprise (5,001 or more employees) had the highest adoption rate of cloud strategies at 40 percent and 35 percent respectively. Only 18 percent of companies with employees between 501-5000 had a cloud strategy in place. The Americas region is a little behind than its EMEA and APAC counterparts in terms of having a cloud strategy in place. 28 percent of companies in the Americas had an existing cloud strategy while the EMEA and APAC regions responded at 35 percent and 41 percent respectively.

Private and Public Cloud Strategies

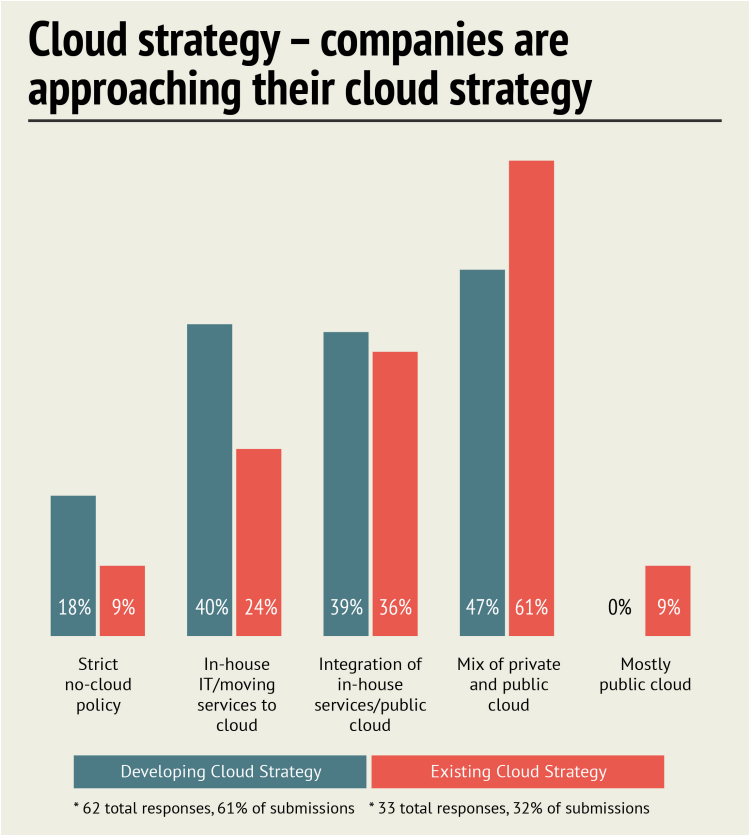


The financial industry is still in the early stages of cloud adoption. A majority, 61 percent of financial institutions, is developing a cloud strategy within their organization. The most common strategies use a mix of private, public, or hybrid cloud environments. The exact deployment models companies took are correlated to the maturity of their cloud strategies. Only nine percent of respondents with existing cloud policies reported predominate usage of private clouds. Financial companies utilizing cloud are using public clouds, while many other companies are utilizing both private and public clouds, with a large percentage actively taking on integration of in-house services with public cloud environments. Companies developing their cloud strategies do not plan on relying as heavily on public clouds. Additionally, 18 percent of the companies still working towards cloud development plan on using a private cloud only model. That is double the percentage of companies that are actually only using private clouds only. These two statistics show added comfort and assurance when practicing in the cloud and is an encouraging sign of maturity in cloud confidence

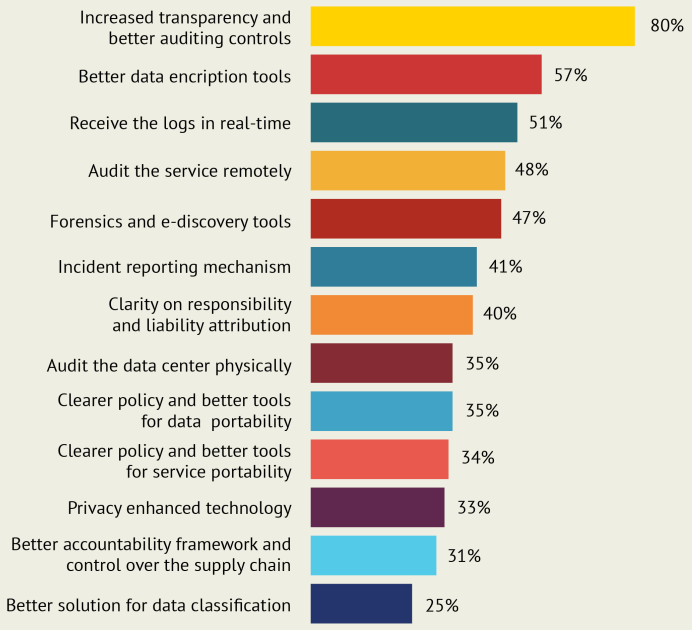
For those that have a strict private cloud only policy, the main reasons are:

- Security concerns (86%)
- Compliance concerns (86%)
- Privacy (79%)
- Data retention and destruction (79%)
- Data residency (57%)

As the mix of in-house IT, private, and public clouds were the most common approach to cloud, it's interesting to note that 70 percent of the companies with existing cloud strategies have moved from hybrid clouds to either a mix of private and public cloud or mostly public cloud. This is another sign of a growing confidence in adopting cloud services and relying less on in-house IT. Having a flexible infrastructure, reduced time for provisioning, reduced total cost of ownership, and shorter time to market are some of the primary reasons for cloud adoption.



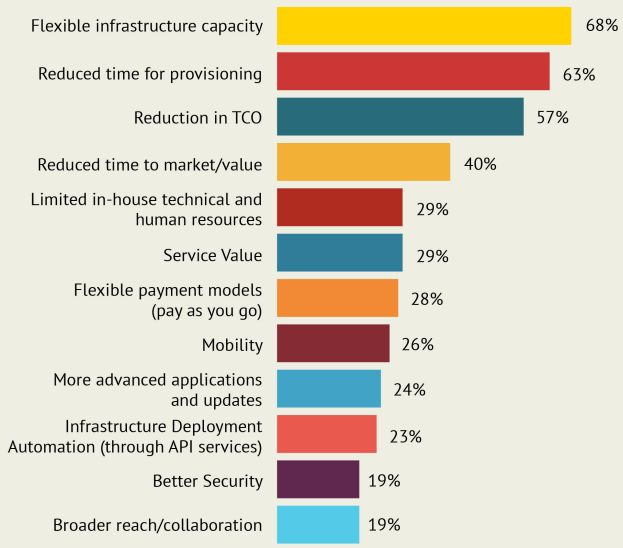
Top Features Desired from Cloud Providers



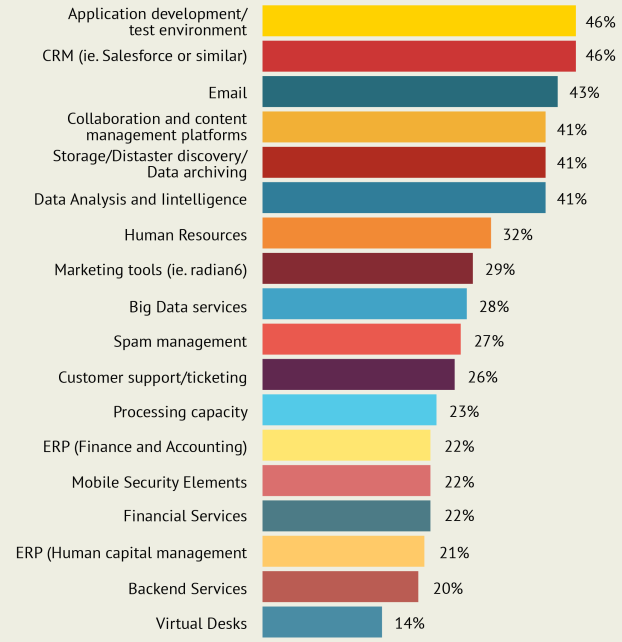
A company's willingness to adopt the cloud has much to do with whether the cloud services offer specific functions and features critical to the users. Some of these features and functions are needed for security and compliance reasons. The top-desired features, reported by our respondents, is "increased transparency and better auditing controls" (80 percent). Better data encryption tools (57 percent), receiving logs in real-time (51 percent), remote auditing (48 percent), and forensics and e-discovery tools (47 percent) lead the remaining top requests. The service itself and, more importantly, how the cloud provider accommodates these top features will determine how readily a particular cloud service is embraced.

The top cloud services/applications that are being adopted provide a snapshot into what organizations are leveraging from current cloud providers. Customer Relationship Management (CRM) tools (46 percent), application development/testing environments (46 percent), and email (43 percent) not too surprisingly led the way. Collaboration platforms (41 percent), storage capabilities (41 percent), and data intelligence (41 percent) are also popular cloud applications. Not a single cloud application category has been adopted by a majority of our survey respondents, which suggests that the business cloud market has substantial growth ahead.

Primary reason for adopting cloud computing



Top Cloud Applications Adopted



Data Security Concerns at the Forefront for Cloud Users

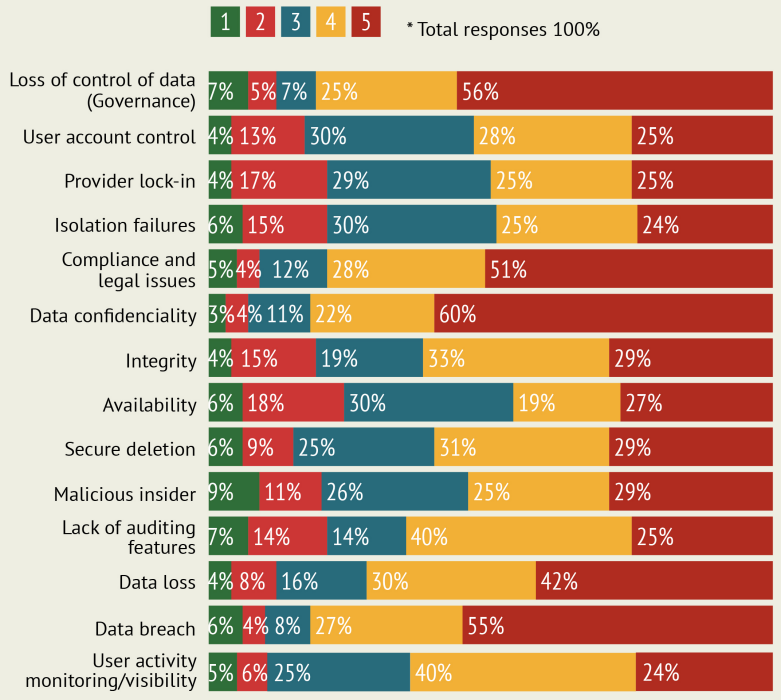
Our study shows a continued concern over security issues relate to cloud. 43 percent of companies considered public breach notification as one of the top obstacles in adopting cloud. 13 percent reported a cloud-related security incident. In particular, data security was the most commonly cited area of concern for the reported incidents: Data availability and leakage was reported in 50 percent of the cloud incidents with 33 percent unauthorized access, 25 percent experienced malware and other vulnerabilities in their breaches, and 17 percent reported service abuse.

When it comes to not adopting cloud, the top reasons reported by our respondents were:

- Security concerns (100%)
- Regulatory restrictions (71%)
- Concerns over public breach notification (43%)

With security concerns being the unanimous barrier holding back cloud adoption, we asked our respondents to rank a list of common security concerns. The respondents ranked each item of concern on a scale of one to five with five being the greatest concern. Once again, concerns over the confidentiality of data and the control of data took the top positions: 60 percent of financial institutions ranked data confidentiality as their highest security concern, followed by loss of control of data (57 percent), and data breach (55 percent). Of the top five highest ranked concerns, the only one that wasn't data-related was legal and compliance issues (51 percent). Each of the issues represents an opportunity for cloud and technology providers to strengthen their offerings to enable financial services firms to better leverage the power of cloud computing.

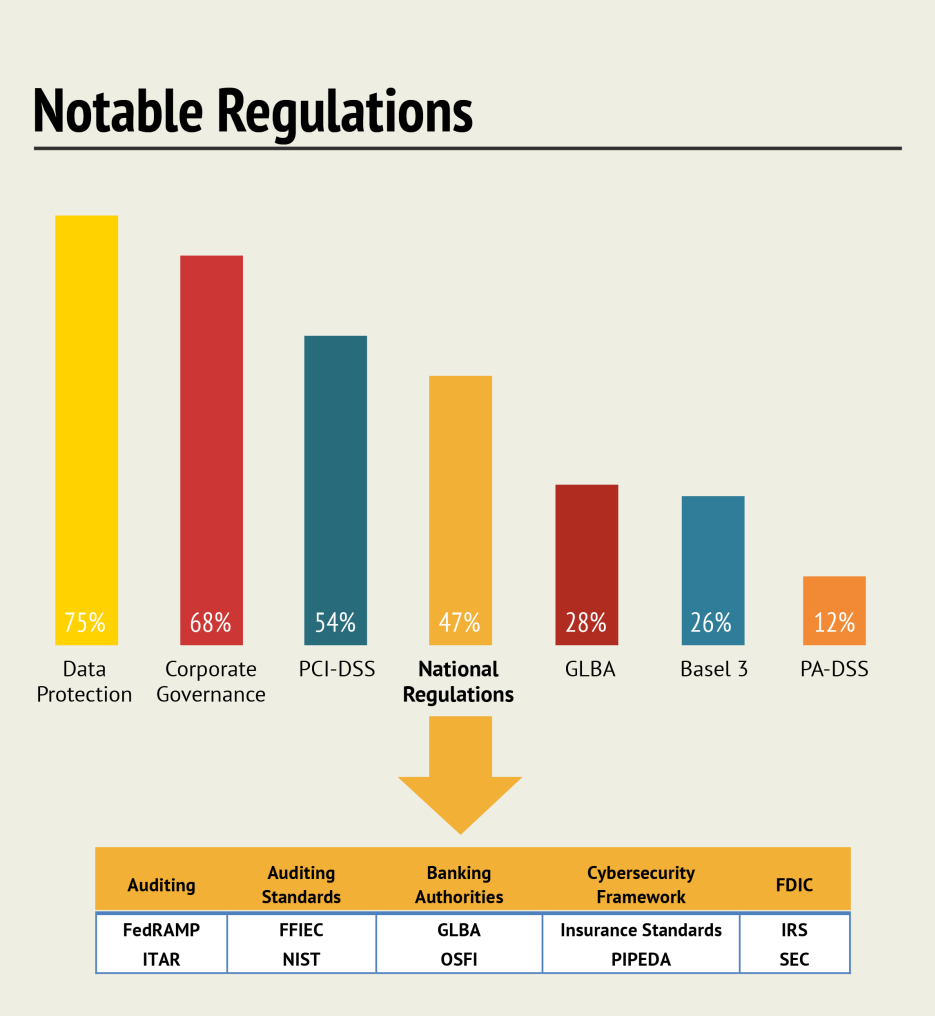
Cloud computing security concerns ranked



Compliance

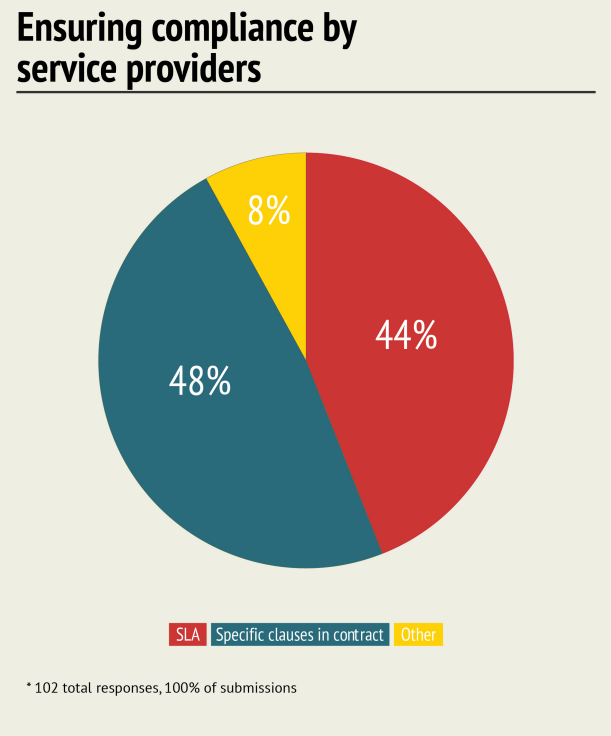
Regulatory restrictions are another top obstacle for companies moving to the cloud. 71 percent of financial companies consider compliance as a reason to keep controls in-house and not migrate data to public cloud services. 31 percent of survey participants indicated they have engaged with regulatory bodies in requirement discussions for the financial sector. More financial institutions are following specific regulations and standards to govern the migration to the cloud. These specific regulations requirements include:

To derive further insights into regulatory compliance, we asked our respondents to rank specific measures they consider critical to achieving compliance while moving to the cloud. The top responses include malware detection, audit permissions, and encryption/tokenization of data. Below is the ranked list of top measures:



- Thorough implementation of security measures (malware detection and removal, forensic readiness, etc.) (66%)
- Auditing permission for incidents (57%)
- Encryption of data at rest (46%)
- Encryption or tokenization of data (and business to retain keys) (46%)
- Penalty clauses for incidents (42%)
- No customer client data in cloud (20%)

As compliance is a crucial operating requirement with banking and financial institutions, cloud adoption must be considered within the context of maintaining regulatory and policy compliance. The study found that companies typically approach compliance assurance with cloud providers through these means: specific contract clauses (48 percent), SLAs (44 percent), and audits (eight percent). The CSA Cloud Controls Matrix is a commonly used tool for compliance in these areas. Additionally, compliance is being enforced by the use of custom audit policies in 18 percent of financial institutions for in-house policies, code reviews, and testing of cloud vulnerabilities amongst others.

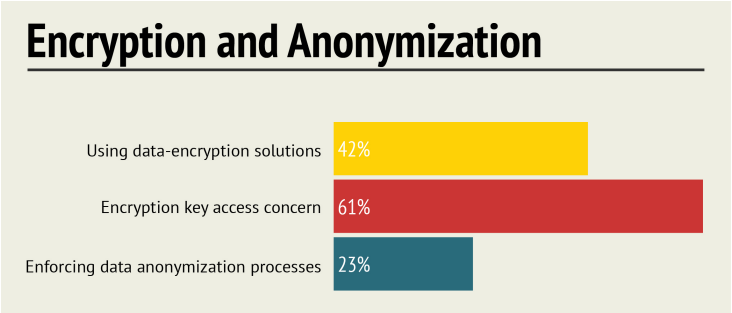


Encryption and Tokenization

As data protection is a common concern for companies considering cloud services, encryption and tokenization functions emerged as top security tools required by financial institutions.

Both early adopters and prospective users of cloud desire encryption capabilities; however, only 42 percent of respondents actually implemented data encryption solutions for the cloud. 61 percent reported that ownership of the encryption keys is a concern. As critical data must be kept confidential, access to the encryption key implies access to the data. As such, enterprises often prefer owning the keys outright on-premises rather than being hosted in the cloud.

As for data anonymization techniques, such as tokenization or masking, fewer organizations (23 percent) are currently deploying such measures when migrating to the cloud. Tokenization and masking are often used to protect critical customer information, PIIs, PHIs, and also data with specific residency constraints.



We see that encryption and tokenization continue to play a critical role in the financial industry, both for securing in-house computing and for migration to the cloud. We expect to see deployment numbers rise in the future as a result.

Key Findings and Summary

Infrastructure flexibility, reduced total cost of ownership, and shortened time to market are just some of the top reasons to move to the cloud. While cloud computing is becoming more and more prevalent throughout the financial industry, companies need to properly weigh the benefits and risks of cloud computing. The study found that most of the industry has yet to build a solidified, concerted approach to cloud adoption and security remains a top barrier. Respondents of the study demanded more visibility, quicker access to logs, and better protection for their data. Cloud providers need to work with financial institutions to better understand how to accommodate these requirements and any specific industry regulations.

As better tools for auditing and data protection become more mainstream, companies will feel more comfortable moving critical data to the cloud, while maintaining its security and compliance posture. Proper guidance and a deeper understanding of the division of security responsibilities between cloud providers and enterprises will build greater confidence leading to wider adoption of cloud services in the financial sector.

About the Cloud Security Alliance

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at http://www.cloudsecurityalliance.org/, and follow us on Twitter @cloudsa.

About CipherCloud

CipherCloud, the leader in cloud visibility and data protection, delivers cloud adoption while ensuring security, compliance and control. CipherCloud's open platform provides comprehensive cloud application discovery and risk assessment, data protection – searchable strong encryption, tokenization, data loss prevention, key management and malware detection – and extensive user activity and anomaly monitoring services. CipherCloud has experienced exceptional growth and success with over 3 million of business users, across 11 different industries. The CipherCloud product portfolio protects popular cloud applications out-of-the-box such as Salesforce, Box, Microsoft Office 365, and ServiceNow.

CipherCloud, named as SC Magazine's Best Product of the Year, technology is FIPS 140-2 validated and is backed by premier venture capital firms Transamerica Ventures, Andreessen Horowitz, Delta Partners, and T-Venture, the venture capital arm of Deutsche Telekom. For more information, visit www.ciphercloud.com and follow us on Twitter @ciphercloud.