TECH COLLABORATORS

Data Security, Integrity and Accessibility in the Cloud

Shared Responsibility Principles for Financial Services Institutions & Cloud Service Providers

Introduction

This document presents principles intended to advance the mission of the Financial Services Roundtable's Technology Collaborators working group on Data Security, Integrity, and Accessibility in the Cloud.

Financial institutions' (FIs) interest in transitioning from legacy computing platforms to the cloud continues to grow. Cloud computing offers operational efficiencies, can help strengthen security and resiliency, and can represent an ability to quickly provide capabilities to the business that improve the delivery of products and services.

FIs looking to leverage cloud services, must consider and assess the Cloud Service Provider's (CSP's) ability and commitment to support the FI's compliance with applicable regulatory requirements, inclusive of requirements specific to third party risk management. While these requirements are not the direct responsibility of the CSP, the CSP's partnership is critical, particularly where security, service quality, and service reliability are concerned.

The following principles were developed jointly by leading cloud service providers and financial institutions to discuss the balance of responsibilities between FIs and CSPs in promoting safe cloud adoption and usage.

The principles address cross-cutting areas of concern that impact data security, integrity, and accessibility and are intended to assist financial services company executives as they evaluate CSPs. Adoption of these principles by FIs and CSPs demonstrates commitment to addressing the above concerns, as well as regulatory compliance as it pertains to data security and data privacy.

Principle 1: Cloud Migrations Depend Upon Trust and Transparency

Establishing trust and transparency between the CSP and FI is critical. Trust is not inherent in the relationship, rather it must be developed through dialogue about the CSP's capabilities and the FI's needs. This dialogue should drive the cloud migration process from its earliest stages.

1. As with all of their operations, when migrating to cloud services, FIs must adopt sound and responsive risk management frameworks such as NIST Cloud Computing Synopsis and Recommendations (Special Publication 800-146, May 2012) and PCI DSS Cloud Computing Guidelines (February 2013) to address compliance, security and performance requirements.

2. There are a variety of deployment models for cloud computing services. FIs may want to consider procuring cloud computing services from a CSP that offers a broad range of service offerings, which can include private cloud, public cloud, community cloud and hybrid cloud, to ensure that the CSP has flexibility to meet the FI's changing requirements over time.

3. As part of the due diligence process, FIs should ensure that they understand the strengths and any weaknesses of each deployment model and the specific configuration being proposed by the CSP to determine whether it is suitable for the FI's purposes and can support regulatory and other obligations.

4. CSPs should make available the information required to support the FI's due diligence and assessment including periodic access to certification, attestation and continuous monitoring documentation. Additionally, allowances should be in place for periodic on-site visits and meetings with CSP teams.

5. The cloud migration process should involve substantive discussions and clear articulation of limitations on the CSP's use and access to FI data.

a. Legal/regulatory – In many jurisdictions, the FI must ensure (typically by contract) that the CSP's use of the FI's data is limited. Limitations may include one or more of the following:

i. The CSP is not able to use the FI's data for any purpose other than that which is necessary to provide the cloud services.

ii. The CSP is expressly prohibited from using the FI's data for unauthorized purposes, such as marketing or more direct client contact without specific agreement.

b. Contractual

i. The CSP should commit in the cloud contract that it will not use the FI's data for any purpose other than to meet the CSP's obligations under the cloud contract.

ii. The CSP should commit to apply strict access controls, with access limited to those within the CSP who require data access to provide the cloud services.

iii. The cloud contract should indicate whether third party contractors or agents (such as hosting services) may have access to the FI's data.

iv. The FI should ensure any click wrap privacy notice and terms of service are consistent with expectations and requirements.

v. Ownership of data and intellectual property should be addressed in the cloud contract.

vi. The CSP should commit, contractually or otherwise, to audit rights for the FI to demonstrate compliance with relevant security standards and other certification regimes applicable to the financial services industry.

6. Service level expectations, commitments and ongoing review should be adequately documented and monitored.

7. To facilitate disaster recovery, the CSP should be transparent regarding the recovery solutions available. The FI should consider the criticality of the data that must be protected and work with the CSP to select high-resilience deployment options.

8. The FI and CSP should agree on breach notification guidelines such as customer notification procedures.

9. The cloud migration process should include discussion and consideration of how the CSP will support the FI's ability to comply with regulatory requirements for security and data protection. This should include, but may not be limited to:

a. Documenting security controls and a commitment to mitigating gaps until necessary controls are implemented, including the formalization of joint meetings and review sessions with a goal of building trusted partnerships.

b. Data management, including what must remain under an FI's control, data portability, data formatting, multi-user tenancy, data segregation, data recoverability, etc.

c. The extent to which third party contractors (CSP subcontracting) may be used and provide for subcontractors to be subject to equivalent security controls as the CSP.

d. Termination procedures such as termination associated with regulatory or supervisory requirements and agreement on the destruction, removal or return of FI data.

e. Other factors for consideration may include, CSP attestation to access management, privileged user access, investigative support, loss of control, and dispute resolution.

Principle 2: Cloud Security Responsibilities Are Allocated Between CSPs and FIs

Cloud security is a shared responsibility that requires cooperation between the FI and the CSP. Financial services customers need assurance that their private information stored, processed and communicated in the cloud will not be used or disclosed in unexpected ways. Privacy controls and policies that are appropriate for financial services customers should be developed, deployed and disclosed.

1. The lines of responsibility and accountability for implementation, operation and management of security controls differ for each service model.

2. The main distinction between service models relates to how control is shared between the FI and CSP, which impacts the level of responsibility for both parties.

   a. The FI rarely has any control over hardware, and the degree to which virtual components, applications and software are managed by the different parties differentiates the service models.

   b. The level of security responsibility generally migrates towards the FI as the FI moves from a SaaS model (Software as a Service, least user responsibility) to an IaaS model (Infrastructure as a Service, most user responsibility).

      i. SaaS: The FI may have limited control of user-specific application configuration settings.

      ii. PaaS: The FI has control over the deployed applications and possibly configuration settings for the application-hosting environment.

      iii. IaaS: The FI has control over operating systems, storage, deployed applications and possibly limited control of certain networking components, such as host firewalls.

   c. The following figure shows how control typically is shared between the CSP and the FI (user) across different service models.

CLOUD LAYER	SERVICE MODELS		
	IaaS	PaaS	SaaS
Applications	User	User	CSP
Interfaces (APIs, GUIs)	User	User	Both
Data	User	User	CSP
Runtime	User	CSP	CSP
Middleware	User	CSP	CSP
Operating system	User	CSP	CSP
Virtualization	CSP	CSP	CSP
Hypervisors	CSP	CSP	CSP
Servers	CSP	CSP	CSP
Data storage	CSP	CSP	CSP
Networking	CSP	CSP	CSP
Physical facilities/data centers	CSP	CSP	CSP

Source: *PCI Security Standards Council, Information Supplement: PCI DSS Cloud Computing Guidelines (February 2013), page 11. (See links to other shared responsibilities models in the support section on page 6.)*

3. The figure above describes the typical responsibilities in a general manner. The details of what is and what is not included in a particular service will vary between CSPs, even if they use the same term (IaaS, PaaS, or SaaS) to identify the service.

   a. Some CSPs offer multiple options for their services, such as one IaaS offering with a user-controlled hypervisor (virtual machine monitor or host machine) and another IaaS offering with no user access to the hypervisor.

   b. Even where an FI does not have control over a particular layer, they may still have some responsibility for the configurations or settings that the CSP maintains on their behalf such as defining firewall rules and reviewing rule sets for firewalls, protecting the user's environment where the CSP configures and manages the firewalls, reviewing and approving user access permissions where the CSP configures access, etc.

4. Where the CSP maintains responsibility for security, the user remains responsible for monitoring the CSP's ongoing compliance with all applicable user requirements. The CSP should provide the means and/or access necessary for the FI to perform such ongoing monitoring of the CSP.

5. To ensure that the required security measures are being met and maintained by the CSP for the duration of the agreement:

   a. The FI should obtain and use implementation guidance from the CSP to help determine how responsibilities are allocated.

   b. FIs and CSPs should clearly document and understand where the boundaries are in their particular relationship rather than assuming that a particular responsibility model applies to them. Clear responsibilities for operation, management and reporting need to be defined for each security requirement.

c. The FI should understand, document and include in the agreement the level of oversight or visibility they will have into security functions outside their control.

d. The FI should design and implement relevant verification of key security controls under the CSP's partial or full control, including via SOC 2 reports or other third-party validation.

Principle 3: Cloud Resilience Depends Upon Cloud Architecture and User Configurations

Both FIs and CSPs face particular resilience expectations in technology deployments. These must be effectively addressed to assure continuous service availability and security for FI clients. Resilience has been described as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions…[including] the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[1]

1. For FIs, the Federal Financial Institutions Examination Council (FFIEC – consisting of the Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau) in their rules and guidance has identified special resilience considerations pertaining to technology service providers [2], covering third party management including capacity planning, testing and cyber events.

2. CSPs that support FIs often need to address expectations about the CSP's preparation for "black swan" scenarios (high impact, hard to predict events) that would significantly test service availability, such as natural disasters.

3. Cloud computing can offer a more resilient environment than many on premise networks. However, this depends on the CSP's underlying infrastructure and capabilities, the FI's vendor management practices, and a regulatory approach that recognizes a range of methods to enhance the institutional resilience, including the use of cloud computing as resilience-enabling technology.

4. To enable resilience in cloud deployment, CSPs should:

   a. Architect services in a manner that provide a commercially-reasonable level of resilience against the broad range of risks that can compromise service availability, whether technological, natural, or manmade (e.g., cyber-attacks, earthquakes, power outages and human error).

   b. Develop materials and artifacts that demonstrate service resilience.

   c. Provide deployment offerings that deliver a higher level of resilience based on customer needs (e.g., risk tolerance, business criticality, and regulatory obligations).

   d. Continuously invest in improving service resilience across the range of services available in a cloud offering.

5. Likewise, FIs should undertake the following activities to enhance resilience in their cloud deployments:

   a. Include resilience considerations in vendor assessment and management programs.

   b. Choose cloud deployment models that improve upon on-premise resilience (e.g., deeper capacity to withstand attacks) and, where possible, select deployments that exceed standardized models.

   c. Leverage resilience enhancements offered by CSPs (e.g., geo-redundancy in data center selection).

   d. Perform drills to test and verify resilience, scalability, and recovery capabilities and processes.

6. FI's and CSP's should maintain awareness of potential concentration risks, including systemic risks, subcontractor concentration, and reverse systemic risk when a service provider has a number of clients where most or all of those clients come from a single sector of the economy. Concentration risks, if overlooked, can result in unplanned service outages, disruption of service to the FI's customer, brand and reputation damage, poorly planned transitions and other serious consequences.

7. 4th party risks (CSP subcontracting) has become a critical area of review for most regulators in the financial services space and therefore should be mitigated through disclosure combined with confirmed assurances through open monitoring, assessment and mitigation of subcontractor risks.

[1] *https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*

[2] *https://www.ffiec.gov/press/PDF/FFIEC_Appendix_J.pdf*

Conclusions

Cloud services create significant efficiencies for FI's including the faster provisioning of software, access to specialty and/or commodity services, the offloading and management of dedicated physical facilities and related operational expenses, allowing financial services companies to leverage software and services from trusted experts, and taking advantage of the CSP's scale and expertise to effectively source infrastructure requirements and outsource ongoing maintenance to third party providers.

Effectively defining and balancing FI and CSP responsibilities and security tasks will greatly increase the value of cloud services partnerships while providing strong confidence in security, integrity and accessibility for customer data in the cloud.

Adoption of these principles demonstrates commitment to data security, integrity and accessibility, as well as regulatory compliance as it pertains to data security and data privacy. These principles will provide financial services companies with a helpful reference point from which to base their decision and approach to utilizing cloud services, and which CSP will provide the best fit and highest degree of confidence between services and operational fit for each business.

Supporting Resources

Definitions for Cloud Service and Deployment Models

The following definitions are sourced from NIST SP 800-145, The NIST Definition of Cloud Computing (2011):

1. Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

2. Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

3. Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

4. Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

5. Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

6. Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

7. Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

U.S. Regulatory References

Regulatory authorities have become more specific in their requirements for FI's in a number of areas related to the use of CSP's and related effective oversight and governance. These heightened standards include effective risk management and governance, independent internal audit review and Board oversight related to risk management. Areas of particular interest include data governance, security standards (e.g. encryption standards, PII, access controls, distribution, etc.) data use and overall controls and stewardship. These heightened standards are growing in importance and are promulgated by federal, state, industry and international regulators alike.

1. FFIEC IT Subcommittee Statement, Outsourced Cloud Computing (July 2012), http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf

2. OCC Bulletin 2013-29, Third-Party Relationships (Oct. 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

3. FFIEC Outsourcing Technology Services Booklet, June 2004 http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf

Other Resources

PCI security Standards Council
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Amazon Web Services
https://aws.amazon.com/compliance/shared-responsibility-model/

Cloud Service Alliance
https://blog.cloudsecurityalliance.org/2014/11/24/shared-responsibilities-for-security-in-the-cloud-part-1/

Microsoft/Azure
https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

Key Contributors

Bank of the West
BB&T
Cylance
Data Boiler Technologies, LLC
East West Bank
FIS Global
Kersplody
Microsoft
MobileIron, Inc.
MUFG Union Bank, N.A.
State Farm
Wells Fargo & Co.

Supporting Contributors

Bank of Hawaii
BCU
Capital One
Carii
Comerica
FCBanking
Genworth
Iberia Bank
Key Bank
Northern Trust
PNC
Primerica
Prudential FiTeq
Regions Bank
Schwab
Securian
U.S. Bank