May
2018

COUNTING ON THE CLOUD

Implications of Third-Party Vendor Risk on Financial Stability in the Cyber Age

Produced for: Institute of International Finance

Produced by: Suzanne El Sanadi | Xiang Lu | Allia Mohamed | Catherine Novack | Alex Wortman | Xinyue Zhang

Faculty Advisor: Professor Katheryn E. Rosen

Disclaimer

This report was produced for the Institute of International Finance as a graduate school consulting project at Columbia University's School of International and Public Affairs. The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the Institute of International Finance.

Table of Contents

Introduction

The safety and stability of the financial system have been the primary goals of the public and private sectors for the past 100 years, and each crisis has brought with it a wave of reactionary policies and practices. Since the most recent financial crisis in 2008, governments, regulators, and industry have collaborated and consulted to achieve policies and best practices to promote confidence in the global financial system. While regulatory bodies mandate policies around capital adequacy ratios, business continuity plans, cybersecurity, anti-money laundering and data protection, cloud computing is an increasingly critical element of the banking system that has not been appropriately incorporated into various regulatory frameworks.

As banks continue to migrate functions to the cloud, the relationship between cloud service providers (CSPs), an increasingly important third-party vendor, and financial institutions is worth dissecting further. There are legitimate concerns that as banks continue to adopt the cloud, CSPs could act as a transmission channel for cyber risks, which could create systemic threats to the financial system as a whole. The lack of substitutability and dependence on only a handful of CSPs begs the question: is the cloud too big to fail?

This paper, divided into three sections, will first analyze the role of CSPs by summarizing the evolution of the cloud computing market and present findings on how banks are leveraging these services. The second section will offer ways in which banks are assessing the risks associated with the cloud and what unique risks – if any – are posed by cloud adoption. The final section will review globally recognized cyber frameworks, the US regulatory environment for cyber and third-party risks and consider global guidance on cloud adoption and how these can be reflected in the US regulatory environment.

While the benefits and power of cloud computing are apparent, financial institutions hold a great responsibility in what they entrust to the cloud and how they use it. This research seeks to evaluate and assess various risks associated with cloud adoption and present recommendations on how global regulatory bodies, government, CSPs and banks alike can count on the cloud while also promoting financial stability in the cyber age.

Methodology and Key Terminologies

Through field interviews with experts in finance, consulting, information security and financial regulation, we have consolidated insights and opinions on third-party risk at the intersection of cyber risks and financial stability. Review of regulatory and industry literature, information security conferences, and market data has helped shape both private-sector and public sector recommendations for securing financial stability in the cyber age. This paper includes some insights from a cloud service provider but focuses mainly on the concerns, comments, and implications for the US Global Systemically Important Banks (G-SIBs).

In an effort to provide clarity and cohesiveness of terms that sometimes carry varying definitions in both cloud computing and financial spheres, we have generated a lexicon of terms that will be frequently used throughout this paper.

- **The Cloud:** A global network of remote servers that operates as a single ecosystem. These servers have varying functions and are designed to store and manage data, run applications, or deliver content or a

service. When this paper refers to "the cloud" it refers to all kinds of cloud services, including public, private, and hybrid clouds, unless specified.

- **Cloud breach:** An unplanned event where data is compromised and can be accessed by unintended parties. A cloud breach can be caused by malicious attacks, human error, or natural disasters.
- **Cloud downtime event:** An unplanned cloud outage or failure that can be brought on by human error, natural disasters, or a malicious attack. A cloud downtime event can be for any period of time and results in clients not being able to use their cloud services. This paper will use the term cloud outage interchangeably.
- **Cloud incident:** Refers to both downtime events and breaches.
- **Concentration risk:** This paper refers to concentration risk as the measure of how a bank's cloud computing power is distributed among the major CSP, how their services are distributed amongst various facilities within a single CSP and how financial institutional clients are distributed within a single CSP. For example, a bank with a small number of cloud service providers has higher concentration risk and a CSP who hosts many financial institutions on a single server also exhibits higher concentration risk.
- **Cyber Risk:** Refers to the risk of financial loss, damage, or business disruption from the failure, breach or outage of a firm's technological systems. Cyber risk can also be considered a subcategory of operational risk.
- **Fourth-party vendor and fourth-party [vendor] risk:** A fourth-party vendor is a business that provides an auxiliary product or service to a third-party of a client. Fourth-party vendor risk can occur when the vendor experiences business disruptions that have a negative impact on the performance of the third-party vendor which in turn impacts the original client.
- **Operational Risk:** Refers to the risk of financial loss, damage, or business disruption from the breakdown of internal procedures, people, and systems. Operational risk is the remaining risk after accounting for financial risks.
- **Systemic risk:** Refers to the risks that could result in the collapse of the financial system or severely disrupt market operations.
- **Third-party vendor and third-party [vendor] risk:** A third-party vendor is a business that provides an auxiliary product or service to a client. Third-party vendor risk can occur when the vendor experiences business disruptions that have a negative impact on the performance of the client.

Part 1: The Cloud Market and How Banks are Leveraging the Cloud

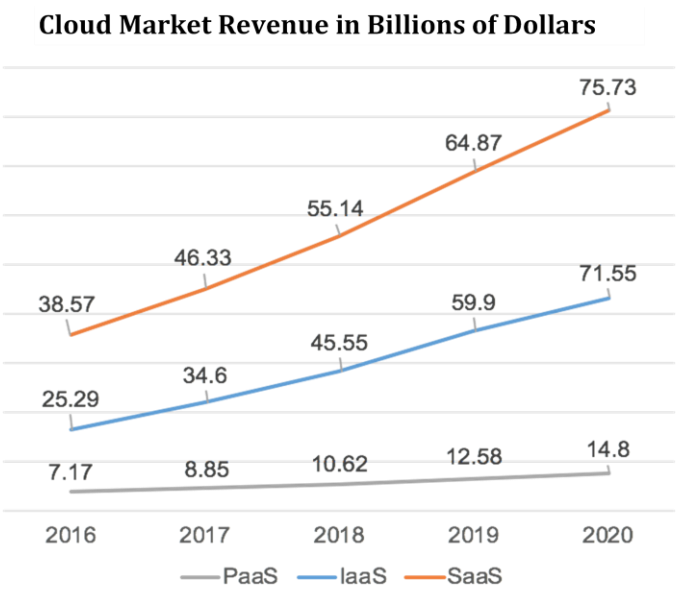
Cloud Market Overview

Cloud computing is the on-demand delivery of computing power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.[1] Since the launch of Amazon EC2 in 2006, the availability of high-capacity networks, low-cost computers, storage devices,

[1] AWS. What is cloud computing?

and widespread adoption of service-oriented architecture and autonomic computing has driven overall growth in the cloud computing market.[2]

Organizations across industries are pursuing cloud strategies because of the multidimensional value that cloud services can provide. The benefits of building applications in the cloud include higher operating efficiency, lower development costs, automatic scaling, and faster provisioning. The cloud market has experienced dramatic growth in recent years and is expected to reach $162 billion in revenues by 2020, a 128% increase from 2016.[3] While financial clients contribute a small proportion of overall cloud market revenues, they are expected to follow the industry trend toward cloud adoption.



Source: Cameron Coles. "AWS vs Azure vs Google Cloud Market Share 2017. Overview of Cloud Market in 2017 and beyond".

Cloud Service Models

Cloud computing is composed of three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

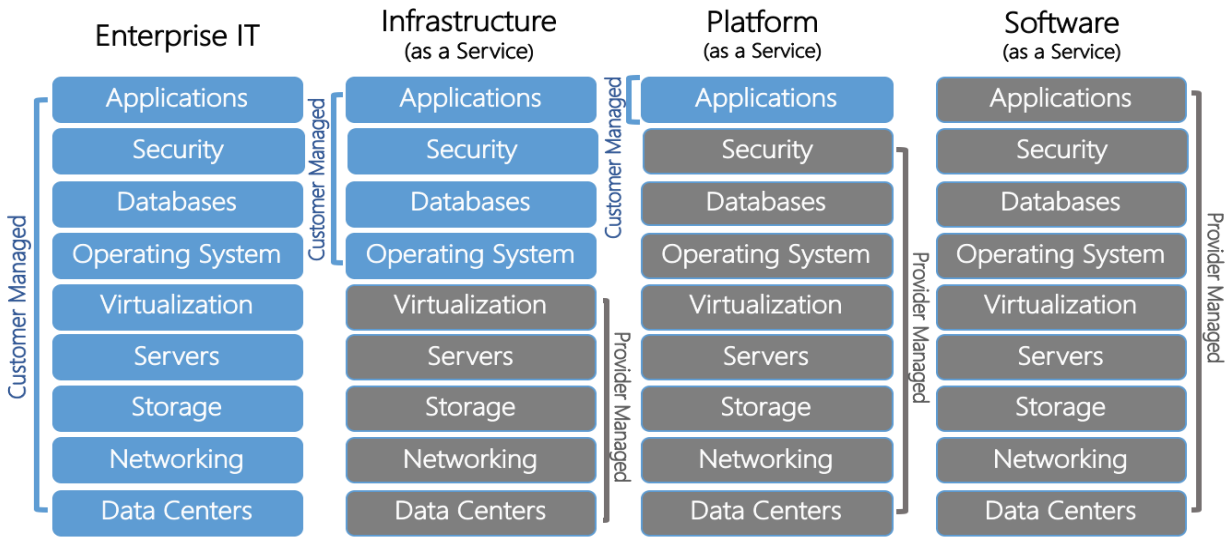
- **IaaS:** Infrastructure as a service (IaaS) provides processing, storage, and network services in a virtual environment. IaaS clients do not control the underlying cloud infrastructure but do have control over deployed applications. The market for IaaS was projected to grow 36.6% in 2017, making it the fastest growing area of all cloud services. IaaS is a baseline service that PaaS and SaaS platforms can be built on.
- **PaaS:** Platform as a service (PaaS) is a category of cloud computing that allows clients to develop and manage applications without building or maintaining any infrastructure. PaaS provides an application development and deployment environment in the cloud by offering the capability of utilizing computer programming languages and tools available from the service provider.[4] Comparing to IaaS, PaaS users cede more of their control power to cloud service providers
- **SaaS:** Software as a service (SaaS) is built on IaaS and PaaS and provides a service that is offered directly to individuals or enterprises. The client does not manage or control the underlying cloud

[2] Gartner. Special Report Examines the Realities and Risks of Cloud Computing. June 2008
[3] Gartner. Report of Cloud Computing. 2017
[4] Cem Gurkok. "Securing Cloud Computing Systems. Overview of System and Network Security: A Comprehensive Introduction"

infrastructure such as networks, servers, operating systems, storage, or even individual application capabilities.[5] SaaS is the top cloud service used by consumers.[6]

The more functions a business outsources to the cloud, the less direct control it has over its IT infrastructure. Clients deploy various cloud strategies and platforms depending on their specific needs. Because SaaS is a "full-service" and user-friendly platform that doesn't require substantial technical expertise, smaller banks are likely to adopt this model, while larger financial institutions would be more drawn to the IaaS platforms.[7]

Descriptions of Cloud Service Models



Source: The Enterprise Cloud Blog. June 2013

Cloud Deployment Models

A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size, and access.[8] The most common deployment models are private, public, and hybrid clouds.

- **Private cloud:** A private cloud exists for a single organization or enterprise and leverages a firm's existing computer servers. In some cases, a private cloud can be hosted by a CSP, which is called a "Virtual Private Cloud"[9]. Regardless if the private cloud is on-premise or off-premise (hosted by a CSP), the services and infrastructure are maintained on a private network that is dedicated solely to one organization.

[5] The Association of Banks in Singapore. "Cloud Computing Implementation Guide for the Financial Industry in Singapore". August 2016
[6] Gartner. Report of Cloud Computing. 2017
[7] Brandon Bulter. How Goldman Sachs and Bank of America use the cloud and containers. December 2015
[8] WhatisCloud.com. "Cloud deploying models". 2018.
[9] AWS. "Amazon Virtual Private Cloud". 2018.

- **Public cloud:** A public cloud is offered by a CSP to multiple clients who share the same cloud infrastructure concurrently. Differing levels of segregation are provided depending on the cloud resources.[10]
- **Hybrid cloud:** A hybrid cloud is a combination of both private and public clouds. The two clouds operate as unique entities but are bound together by standardized technology that enables data and application portability.[11] In a hybrid cloud, data and applications can move between private and public platforms for greater flexibility. For example, banks could use the public cloud for high-volume, lower-security needs and leverage the private cloud for critical or sensitive operations.[12]

Deployment Model's Responsibilities

Deployment Model	Managed by	Owned by	Location	Used by
Public	External CSP	External SCP	Off-Site	Untrusted
Private	client or external CSP	client or external CSP	On-site or off-site	Trusted
Hybrid	client and external CSP	client and external CSP	On-site and off-site	Trusted and untrusted

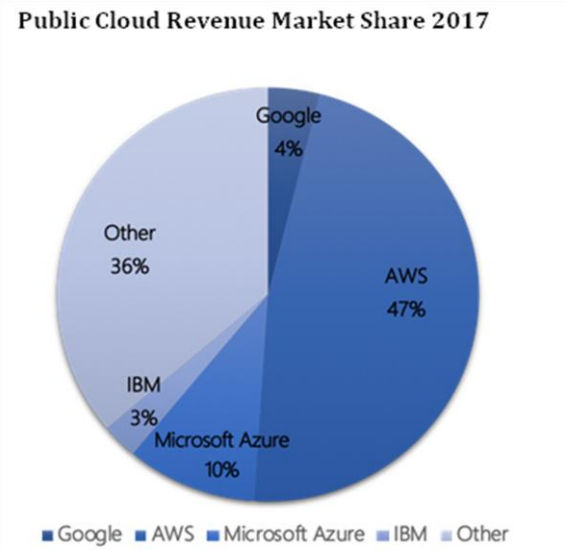
[10] Gurkok, C. "Securing Cloud Computing Systems. Overview of System and Network Security: A Comprehensive Introduction." Network and System Security, Synergess, 2016.
[11] The Association of Banks in Singapore. "Cloud Computing Implementation Guide for the Financial Industry in Singapore". August 2016.
[12] Microsoft Azure. "What are public, private and hybrid cloud?". 2018.

Source: Gurkok, C. "Securing Cloud Computing Systems. Overview of System and Network Security: A Comprehensive Introduction." Network and System Security, Synergess, 2016.

Major Cloud Service Providers

According to Synergy Research, four of the five largest CSPs gained market share in 2017. Amazon Web Service (AWS) is the dominant market leader with 47% market-share, followed by Microsoft Azure, IBM, Google, and Alibaba.[13]

AWS and Microsoft Azure are the two most prominent CSPs among financial institutions. Microsoft reported that "more than 80% of the world's largest banks are Azure clients".[14] Banks are continuing to disclose and comment on their relationships with CSPs, including Bank of America and HSBC.



- **Bank of America (BoA) & Microsoft Azure:** BoA commented on how Microsoft was going to be a part of their strategy to migrate 80% of their technology workloads to virtual platforms, furthering their push to be a digital leader in financial services.[15] BoA is committed to allocating more of their $3 billion annual computing infrastructure budget to the public cloud, following a rapid improvement in security technology.[16]
- **HSBC & Google:** HSBC noted their close relationship with Google in helping them secure a safe route to the cloud that will ensure future seamless migrations. HSBC is aiming for a cloud-first approach to data analytics and machine learning and is keen to outsource the "headache: of managing the massive infrastructure associated with those capabilities.[17]

Trade-Offs: Maximizing Efficiency vs. Concentration Risk

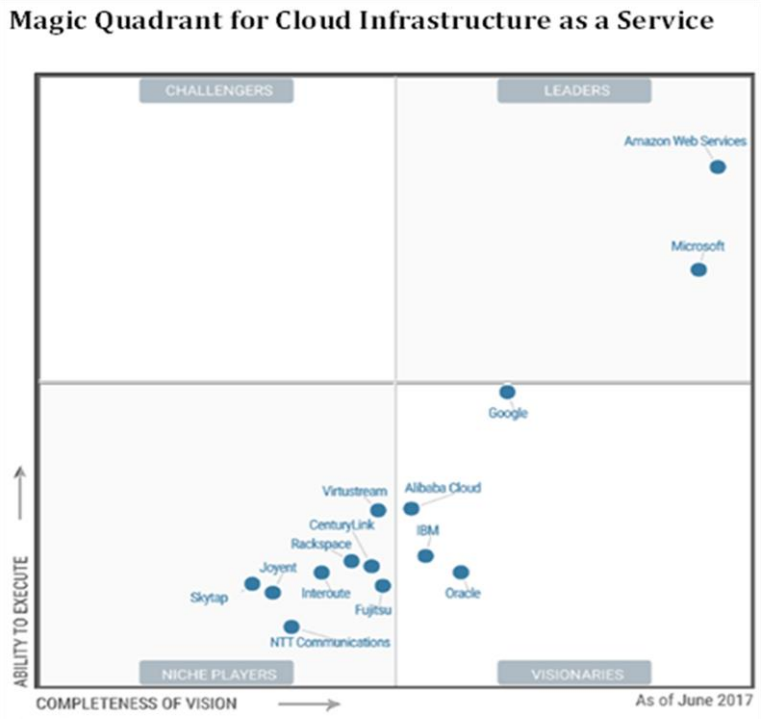
According to a 2017 McKinsey report, more than 75% of organizations surveyed[18] had yet to migrate the majority of their business activities to public-cloud platforms. However, institutions from every industry are expected to double their cloud usage by 2020, from 19% of their workloads to 38%.[19]

Companies are steadily moving their applications and data from on-premise data centers to public-cloud platforms. While managing third-party risks associated with the cloud are at the forefront of IT strategies

[13] Bourne, J. "AWS passes $5 billion in quarterly revenue with a $20bn run rate". Feb 2018
[14] Microsoft. "Earnings Release FY2017 Q4." July 2017.
[15] Microsoft News Center. "Bank of America chooses the Microsoft Cloud to support digital transformation." Oct 2017
[16] WSJ. "Why Amazon and Google Haven't Attacked Banks". April 2018.
[17] Silicon. "HSBC Embraces Google Cloud For Big Data Analytics And Money Laundering Detection". May 2017.
[18] The survey interviewed with cybersecurity executives at 97 enterprises across industries, including financial services and insurance (34%), healthcare (15%), retail and consumer packaged goods (6%), and technology, media, and telecommunications (13%) to see the trend of public cloud adoption.
[19] McKinsey. "Making a secure transition to the public cloud". 2017

for financial institutions[20], banks are willing to accept these challenges due to the extensive benefits of cloud computing.

- **Scalable computing power:** Cloud vendors have implemented auto-scaling to enable users to automatically increase capacity when additional performance is needed and scale down when demand subsides.[21]
- **Further privacy and security:** Financial institutions that utilize CSPs for client analytics, data storage, asset and wealth management, and other functions can create "private" segments by using encryption technologies tailored to their specific circumstances. Encryption keys are managed by banks themselves, which secures access to client data. Within the public cloud, banks can still maintain significant control of their functions and data. To some extent, the security posture of major CSPs can be better than most enterprise data centers or in-house private cloud.[22]
- **Lower cost and higher efficiency:** With cloud computing, financial institutions can transform what would be a large up-front capital expenditure into a smaller, ongoing operational cost. The public cloud enables instant experimentation, immediate results, and an efficient exit, creating a dynamic culture where banks can test virtually any scenario or new software tool without the expensive provisioning cycle.[23]
- **Business continuity:** Financial firms can leverage the cloud as an efficient and cost-effective backup solution.[24] In the event of a cloud outage, banks can transfer operations to another cloud server within a CSP, pass over functionalities to another CSP, or bring on-premises.



Source: Gartner, 2017.

[20] PwC. "Financial Services Technology 2020 and Beyond: Embracing disruption." 2016.
[21] DTCC. "Moving Financial Market Infrastructure to the Cloud, Realizing the Risk Reduction and Cost Efficiency Vision While Achieving Public Policy Goals". May 2017
[22] Gartner. "Clouds Are Secure: Are You Using Them Securely?". Sep 2015
[23] DTCC. "Moving Financial Market Infrastructure to the Cloud, Realizing the Risk Reduction and Cost Efficiency Vision While Achieving Public Policy Goals". May 2017
[24] Capgemini. Cloud Computing in Banking: what banks need to know when considering a move to the cloud?

Despite the apparent benefits of the public cloud, some financial institutions still deploy private cloud models because of data protection concerns or third-party risk aversion. Some governments have also established considerable barriers for firms wanting to migrate client data to a public cloud.[25] In-house private clouds in many cases cannot provide the same level of scalability as the public cloud which will continue to drive adoption amongst financial institutions despite their risk aversion.[26]

Magic Quadrant Reveals Concentrations Risk

Gartner published a magic quadrant for infrastructure-as-a-service (IaaS) that has Amazon Web Services and Microsoft in the leader's quadrant with Google a trailing third rank.

These top three CSPs dominate the majority of the cloud-services market, which significantly increases clients' exposure to concentration risk. Concentration risk can occur at both industry-level and firm-level. At the industry-level, if G-SIBs rely on the same vendor for their services, the entire financial industry could be vulnerable if that one CSP is compromised with a breach or outage. This [illegible]evel concentration risk is a concern as the financial industry continues to adopt the cloud and bigger banks influence their peers to update IT infrastructures. At the firm-level, a bank that uses only one CSP or house all of their functions on one server within a single CSP also face concentration risk in the event of cloud outage or breach.

Concentration risk has been addressed by some market experts and in several industry reports but has not been fully explored as a systemic risk to the financial system. One reason might be concentration risk is still relatively small because banks are still "doing a lot internally" and are not leveraging the cloud for critical business functions.[27] However, it is estimated that by 2020, core service infrastructures in areas such as consumer payments, credit scoring, and statements and billings will likely to be transferred to the cloud.[28] Given this trend, both financial institutions and regulatory bodies will be forced to look at concentration risk mitigation in what will be a cloud-dominant future.

Financial Institutions and their Journey to the Cloud

For the past decade, financial institutions have been deploying cloud computing services with limited transparency to their clients, market participants, regulators, and other stakeholders. Currently, there is no publicly available information as to what and how much banks are putting on the cloud, what security measures they have in place, and what CSPs they are using. Because the relationship between financial institutions and CSPs is relatively new, market participants have been ignorant to various cloud outages and cyber events and what impact these events can have on bank functions and the financial system as a whole.

[25] PwC. "Financial Services Technology 2020 and Beyond: Embracing disruption"
[26] Symmetry. Virtual Private Cloud vs Private Cloud: What's the difference?
[27] W. Kuan Hon, Christopher Millard. Banking in the cloud: Part 2 – regulation of cloud as 'outsourcing'.
[28] PwC. "Financial Services Technology 2020 and Beyond: Embracing disruption"

Cloud Outages and How They Can Impact Financial Institutions

In the past decade, there have been numerous cloud outages (or downtime events) as the result of malicious attacks, human error and natural disasters. In March 2018, a power-outage impacted Amazon Web Services' (AWS) US-East 1 region, one of its largest, and the subsequent cloud outage affected hundreds of notable enterprise services such as Atlassian, Slack, and Twilio[29]. This outage generated no media attention or negative stock price movement for Amazon, as the outage lasted just 18 minutes. The muted stock price movement solidifies the notion that market participants are not paying attention to the relationship between financial institutions and cloud providers due to lack of transparency and knowledge of what the possible implications are to the financial system. Without this transparency, market participants will be unable to hold banks and CSPs accountable in the event of a major cloud outage. While this downtime event was unremarkable to both markets or media outlets, it's evident an 18-minute outage could cause concerning losses for market participants that have become dependent on a variety of cloud computing services. According to a 2018 report by Lloyd's, a cyber incident that would take a top three cloud provider offline for 3-6 days could result in up to $15 billion in business interruption losses in the US, but just $450 million in losses for the finance and insurance industries[30].

How Banks are Leveraging the Cloud

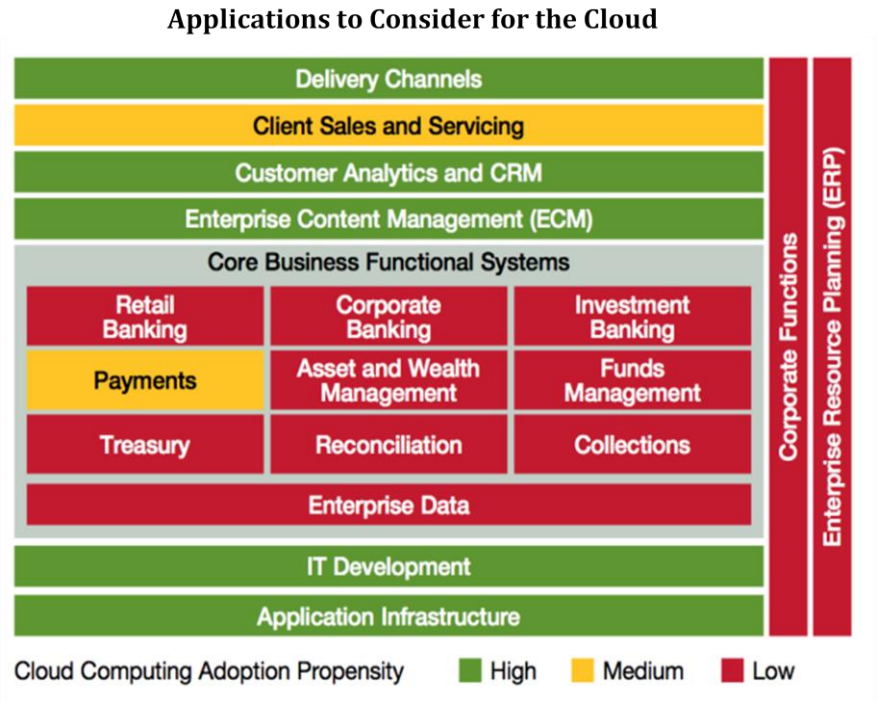
One of the main factors shielding the financial industry from greater losses is what they choose to put on the cloud. CapGemini analysis looked at various banking business lines and its propensity for cloud adoption and concluded that non-core business segments such as client analytics and IT development were better suited for the cloud, while core functions such as retail banking and asset management would pose more challenges[31]. Based on our interviews with executive information security officers at several financial institutions, it is apparent that banks have been highly selective in what they entrust to the cloud so far, and conservatively deploy a mix of both public and private cloud services.

Banks are leveraging a variety of cloud services including grid computing, data analytics, disaster recovery initiatives, and digital transformation projects. Entities like Coinbase and FINRA deploy the cloud for analyzing millions of transactions, while the National Bank of Canada uses the cloud to more efficiently process historical market data to improve their algorithmic trading[32]. Capital One is one of Amazon's largest bank clients and is experimenting with virtually every AWS offering to "develop, test, build and run its most critical workloads"[33][34]. These case studies corroborate the thesis that financial institutions are moving away from traditional uses of the cloud and deploying more sophisticated services for some of their core business functions, such as trading, payments and funds management.

[29] ThousandEyes. "Amazon AWS Outage a Lesson in Managing Cloud First Risks." March 2018.
[30] Lloyd's & AIR Worldwide. "Cloud Down: Impacts on the US Economy". January 2018.
[31] Capgemini. "Cloud Computing in Banking." July 2017.
[32] AWS. "Financial Services Customer Success Stories," January 2018.
[33] AWS. "Capital One Case Study." January 2018.
[34] Wall Street Journal. "Next Up for Amazon: Checking Accounts." March 2018.

How Financial Technology is Driving Cloud Adoption in Traditional Financial Institutions

The financial industry's conservative deployment of the cloud has helped protect it against various cloud outages over the past decade. It has become apparent, however, that this cannot be a long-term mitigation strategy as the emerging trend toward open banking and innovative pressure from financial technology (FinTech) firms pushes banks to more robustly adopt the cloud. The European Commission's FinTech Action Plan emphasized how FinTech-based solutions that leverage the cloud can provide better access to finance and improve financial inclusion for digitally connected citizen.[35] A McKinsey report on data sharing and open banking solidifies the notion that many financial technology firms are revolutionizing financial services, forcing the traditional financial sector to innovate and possibly leverage technologies such as cloud computing, artificial intelligence, and blockchain and application programming interfaces (APIs).[36]



Source: Capgemini, 2017.

In the past decade, traditional financial institutions such as Citi, JP Morgan and Goldman Sachs, have established venture capital and strategic investment groups to source innovative financial technology firms.[37] Legacy technologies that are critical to the capital markets ecosystem are roughly 40 years old and are stifling market innovation. Banks are quickly realizing that in order to maintain competitiveness, they need to leverage emerging technologies including the cloud. This sentiment is solidified in recent quarterly earnings calls, where the prominence of the word "digitization" has increased 250% over the course of 2017 for banks such as Bank of America, Wells Fargo, and Citibank.[38] Mizuho Bank, among other international banks, is also showcasing a commitment to their clients' digital experience through their API bank initiative, which operates on IBM's Cloud platform. The initiative is meant to connect internet banking with other fintech innovations through applications, such as balance inquiry and payments[39].

[35] European Commission. "FinTech Action Plan: For a more competitive and innovative European financial sector." March 2018.
[36] McKinsey & Company. "Data Sharing and Open Banking." September 2017.
[37] CBInsights. "Banks in FinTech: What's Ahead in 2018". January 2018.
[38] CBInsights. "Banks in FinTech: What's Ahead in 2018". January 2018.
[39] IBM. "Mizuho Bank Begins API Banking on IBM Cloud to Help Drive Innovation with Partners". June 2017.

For the past few years, G-SIBs have actively participated in venture rounds of prominent FinTech firms that are dedicated to market infrastructure. Both US and European banks have jointly invested in over a dozen capital markets infrastructure companies since 2012[40]. Most recently in August 2017, Goldman Sachs participated in a $45 million Series E investment for Skytap, a cloud provider that specializes in the migration and modernization of core business applications to the cloud.[41] This investment could imply that Goldman Sachs is starting its due diligence on cloud migration support as they prepare to build out their own cloud platforms. Another example of this emerging trend is Starling Bank, a mobile-only bank in the UK completely built on the cloud.[42] For large financial institutions to maintain competitiveness and retain market share, their cloud adoption strategies will evidently evolve and become more robust over time.

Observations and Analysis

- Cloud adoption is at the forefront of many bank information technology strategies
- Public cloud adoption by financial institutions is inevitable and will become the dominant infrastructure model.
- While AWS, Microsoft Azure, Google, and IBM are still the leading cloud vendors, AWS and Azure are the two most prominent CSPs for financial institutions. As a result, concentration risks can occur at both firm and industry levels.
- Concentration risk has yet to receive the attention it deserves from users and policy makers. Mitigation strategies should be deployed by both banks and regulators.
- However, the security posture of major public cloud providers is still considered more secure than most enterprise-level data centers by many financial institutions. Firms can further upgrade their security levels by leveraging strategies such as encryption keys. If banks are diligent in deploying public cloud infrastructure, developing applications on the cloud could be a more secure option than developing in-house frameworks.
- Taking into account third-party vendor threats, financial institutions are experimenting with various cloud computing services for analytics, payments, and trading.
- Banks will continue to robustly adopt the cloud and migrate core-functions to keep pace with innovative financial technology firms and to take advantage of cost-efficiencies, cloud computing power and the security that major CSPs can provide.

Part 2: Cloud Cyber Risks and Risk Mitigation Strategies

It is evident that banks are increasingly adopting CSP's services for multiple business functions, and that this growing trend generates additional risk. For individual institutions, the technical risks decrease with better computer architecture and network security expertise, but the exposure to operational risk increases as banks relinquish control to third-party vendors, including CSPs. While the financial system can benefit from a more resilient infrastructure provided by CSPs, there are certain "fat tail risks" that must be

[40] CBInsights. "Banks in FinTech: What's Ahead in 2018". January 2018.
[41] Skytap. "Skytap Announces $45 million Series E Led by Goldman Sachs". August 2017.
[42] Quartz. "Amazon is invading finance without really trying". November 2017.

addressed. A cloud-related cybersecurity incident for example could prove to be systemic, which is why it is important to understand the transmission channels through which a cyber event could threaten financial stability.

Cyber Risk Transmission Channels

With regards to the financial system, cyber risks transmission channels exist at both the macro and micro level. The macro level risk relates to how a cyber event can be transmitted to affect the financial system, while the micro level is concerned with how risk is transferred between IT systems. The Office of Financial Research (OFR) has explored this topic at the macro level as it has laid out three channels through which cybersecurity events could threaten financial stability: lack of substitutability, loss of data integrity, and loss of confidence.[43]

- Substitutability is an issue because many critical functions of the financial system rely on the operation of particular institutions. If a cyber event disrupted operability of a utility providing a critical role for a major financial network, for example, it could result in a systemic spillover effect.[44]
- Data integrity is essential for the operation of financial markets, as many transactions run on a just-in-time basis and data corruption or destruction could interrupt banking activity.[45]
- Confidence is the backbone of a banking industry. A loss of confidence can lead to panic that could cause clients to rapidly withdraw funds, also known as a bank run.

The IIF has expanded on this model and described several scenarios where a significant cyber-attack could threaten financial stability through these three channels, such as an attack on payment systems, manipulation of data, and failure of wider infrastructure.[46]

The same model of transmission channels should be considered when assessing financial risk relating to the use of CSPs. The decision to outsource computing operations to third-party cloud providers cedes operational control from the firm. If all G-SIBs migrate critical functions to one or a select few CSPs, there is an issue of substitutability. Similarly, if the data being used in the cloud is compromised, banks could suffer from unintended exposure such as errors in risk calculations. Lastly if consumers lose faith in the security of the cloud and lose confidence in the stability of banking system, then the market could face significant volatility or even a bank run.

Security for cloud computing should follow the same basic standards as traditional network security - the network is only as secure as its weakest link. Cyber transmission of risks within the cloud also follow this principle, where any lapse in traditional security practices could threaten the overall safety of the cloud, as compromised IT systems could transfer malware from clients to the CSPs, and vice-versa. There are some cyber transmission channels at the micro level that are particularly salient to banks outsourcing operations

[43] Office of Financial Research. "Cybersecurity and Financial Stability: Risks and Resilience." February 2017.
[44] Ibid. pg 3.
[45] Ibid. pg 4.
[46] IIF. "Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system." September 2017.

to third-party cloud providers such as messages, data transfers, and computer hardware within the supply chain.

Messages such as email are a common method by which malicious actors transmit malware to gain access into network systems. However, the banking industry also uses specialized application-to-application communications such as SWIFT and Fedwire to communicate between financial firms. Although these applications are supposed to create an additional layer of security, they are not impermeable. In 2016, $81 million was stolen by hackers from the central bank of Bangladesh by abusing the trust generated from the SWIFT software program.[47] CSPs leverage similar messaging applications and channels to communicate with their clients, which should be evaluated and tested to ensure security.

Data Transfers between banks and CSPs presents another transmission channel for cyber risk. According to interviews with major financial firms, some banks are leveraging the cloud to execute risk calculations for their market positions. As a result, banks are continuously transmitting data between their cloud and domestic IT infrastructure which presents increased risks. The banking industry has instituted a number of processes and technologies to minimize data transfer risks, such as data encryption and virtual machine imaging.[48] Furthermore, interviews with regulators suggest that CSPs have been active in implementing robust security measures that are tailored to the specific concerns of the financial sector.

The hardware used for servers is another critical factor when evaluating security. As the supply chain network grows and is less connected to the banking industry, the risks posed by the hardware of vendors become more opaque. While there is existing US regulatory guidance on risk mitigation of third-party relationships[49], many firms are concerned about the fifth-party (or supply chain) risk that relates to the vendors of CSPs. Sourcing of hardware is critical for security especially because nation-state actors have been known to create backdoor surveillance functions within equipment that is exported to strategic sectors abroad.[50] Therefore, quality as well as origin of the product must be considered for security purposes. If vendors further down the supply chain are ignorant to these risks, they could cause unintended consequences for the clients of CSPs.

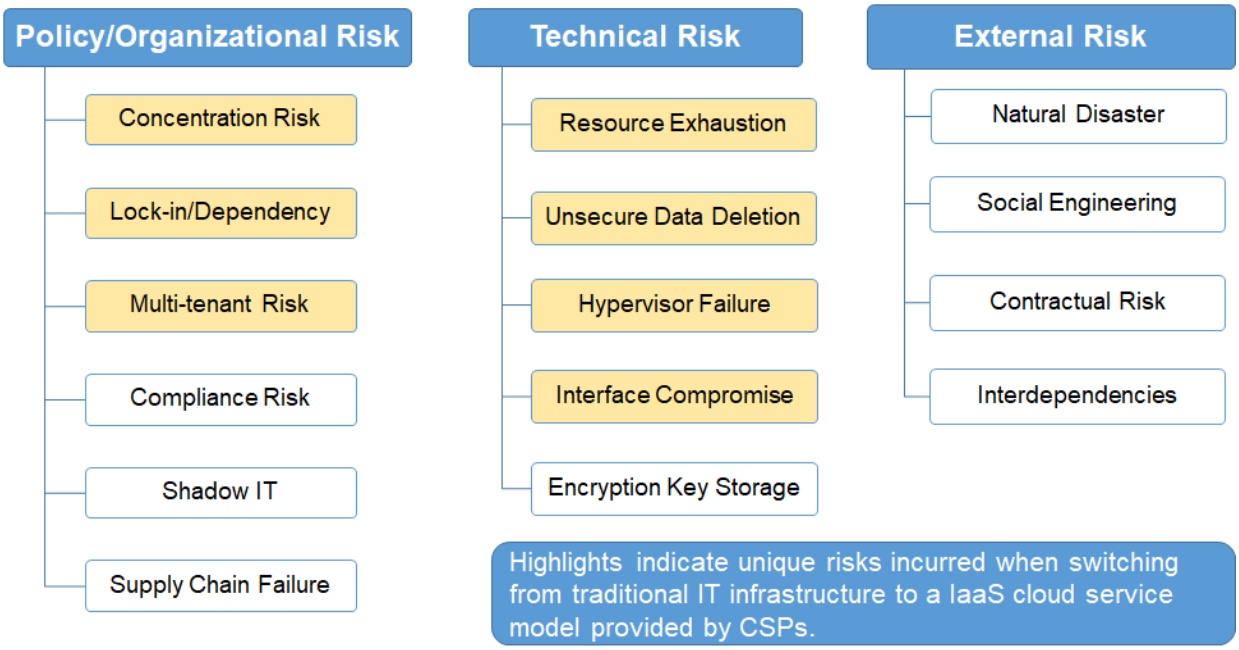
Unique and Escalated Risks for Cloud Computing

Migrating to the cloud provides an opportunity to construct a stronger security environment by redesigning computer architecture and network protocols.[51] Although these capabilities are not unique to the major CSPs, firms such as Amazon and Microsoft have invested heavily in building teams that have the technical expertise and resources to construct more technically secure networks. Despite CSPs strong commitment to security, the switch from traditional IT infrastructure to the cloud can still create and escalate various risks. The nature and degree of the cyber risks posed to financial institutions are dependent on both the

[47] Finkle, J. “Bangladesh Bank hackers compromised SWIFT software, warning issued.” Reuters, April 2016.
[48] Cloud Security Alliance. “Security Guidance for Critical Areas of Focus in Cloud Computing 2.1.” 2009.
[49] OCC. “Bulletin 2013-29: Third-Party Relationships.” October 2013.
[50] Greenwald, G. “Glenn Greenwald: how the NSA tampers with US-made internet routers.” The Guardian, May 2014.
[51] Cloud Security Alliance. “Security Guidance for Critical Areas of Focus in Cloud Computing 2.1.” 2009.

cloud deployment model and cloud service model selected. The financial risk incurred by banks is largely dependent on what functions are outsourced to the cloud and where relevant data is stored and transmitted.

The risks derived from CSPs can be broadly grouped into three categories: Policy & Organizational Risks, Technical Risks, and General Risks. Policy & Organizational Risks describe unique or escalated risks due to a bank's policy decisions relating to its IT organizational structure. Technical risks are those associated with the network architecture of public cloud computing. External Risks are caused by or are dependent on outside forces. This section will examine the unique and escalated risks generated when banks switch from legacy IT data centers to an IaaS platform within a public cloud infrastructure. With the assumption that banks desire to maintain as much control over their security, we chose to do an analysis of the risks associated with IaaS, as this model retains the most control with banks. Furthermore, the risks are categorized into two groups: unique and escalated. Unique risks are those that did not previously exist when using in-house, legacy IT systems. Escalated risks are a function of two variables: impact and probability. Probability is the likelihood of an event occurring while impact is focused on the severity of the potential damage that could occur.



Source: SIPA Capstone Team

Policy & Organizational Risks

Concentration Risk: Unique

As we introduced earlier, a cloud service outage could severely hamper business operations, especially if the firm is reliant on just one single cloud provider. Furthermore, there is an increased chance of financial instability if all major financial institutions are relying on just a few CSPs. If computing power becomes scarce or unavailable, certain operations at banks could cease. Moreover, if the financial system faces extreme pressure, banks may be incentivized to do what is in their best interest, furthering any threat to the

financial system as a whole.[52] As we noted previously, concentration risk exists at both the firm and industry levels.

Lock-in or Dependency: Unique

Dependency risk is established if a bank becomes completely reliant on its cloud provider and has no reasonable alternative or substitute. For example, the bank may find that it is unable to transfer its data to another cloud provider due to incompatible file storage. Another potential instance of lock-in is if CSPs are the only suppliers that can meet a bank's need for computing power. This risk also could put banks in a position where they lose their bargaining power and the CSPs are left in a monopolistic position. We determine that this risk is unique because traditional IT infrastructure does not pose similar threats.

Multi-tenant Risk: Unique

Use of the public cloud means that multiple clients will have access to and will have data stored on the same servers. However, this does not mean that a client will have access to all the data and resources that are being stored on a server, as the CSP should have strong cloud architecture that has appropriately configured client privilege roles. Additionally, CSPs can strengthen security of individual tenants by virtually segmenting operations through the use of a firewall or micro-segmentation.[53] If there is an instance of resource segregation failure, a tenant on a shared infrastructure could be subject to guest-hopping, SQL injections, or side-channel attacks,[54]exposing their sensitive data or resources to unauthorized parties.

Compliance Risk: Escalated (increase probability, increase impact)

Although CSPs have actively engaged with financial firms and regulators to be compliant with financial regulatory requirements, the ability of the cloud to leverage resources and store data in multiple locations increases the complexity of managing compliance, creating additional risk. The environment is further complicated as jurisdictions are creating new laws and rules to manage data storage and transfers, yet without consideration to other dominion. For instance, the General Data Protection Regulation (GDPR) in the European Union has strict rules governing data storage, where severe fines of up to 20 million euros could be levied.[55] At the moment, banks are able to determine the region and sub-regions of the servers they are using for data storage and computing capabilities however, this is managed by the banks and therefore each bank must be aware of how to properly use these tools. Additionally, it is critical that banks actively communicate with CSPs to secure their networks according to security best practices, such as using encryption and employing multiple layers of defense.

Shadow IT: Escalated (increase probability, increase impact)

Cloud computing provides a wealth of additional resources to the employees of the bank, however not all of these resources are equally secure since not all extensions or applications are designed with security in mind. Interviews with banks suggest it is important to have controls that restrict the ability of employees,

[52] Expert Interview with Professor Patricia Mosser regarding financial stability
[53] Cloud Security Alliance. "Security Guidance for Critical Areas of Focus in Cloud Computing 2.1." 2009.
[54] Securing Cloud Computing Systems pg. 99.
[55] EU GDPR. "GDPR Key Changes."

employees of vendors, and software engineers from accessing cloud services that have not been evaluated and approved by management.

Supply Chain Failure: Escalated (increase probability)

Cloud providers also outsource certain tasks relating to constructing and maintaining their cloud network. Therefore, the CSPs security framework must also account for this outsourcing as a lapse in their third-party vendor's security could be transmitted and cause vulnerability within the cloud network. As the parties become more distant from the banking firms, the risk becomes less transparent and thus is harder to manage.

Technical Risks

Resource Exhaustion: Unique

Due to the changing nature of cloud technology, CSPs must be able to predict the future demands for computing resources in order to properly leverage their efficiencies and serve their clients. CSPs model the needs of their clients through statistical projections, and incorrect modeling could lead to a situation where computing demand outweighs computing supply. Another potential risk is that proliferation of malware that compromises networks to siphon their computing power for profit. Most recently, there have been reports of a major cloud provider's management interface being abused to mine for cryptocurrencies.[56]

Unsecure Data Deletion: Unique

Banks that utilize cloud provider services must be able to ensure that the data they put up in the cloud is properly wiped from cloud storage when deleted. Cloud computing by its nature requires physical hardware to be reallocated and data to be stored in multiple locations, but banks usually do not intend to permanently keep this material on the cloud network. Given that much of this information is sensitive, it is vital that banks are able to ensure its deletion so it cannot be restored by other actors.

Hypervisor Failure: Unique

Cloud architecture depends on a specialized service engine known as a "hypervisor". The hypervisor that operates over the physical hardware resources and manages the multiple virtual machines that make up cloud computing. Just as with any operating system, the hypervisor software can have vulnerabilities within its code that could cause unexpected failure or be subject to cyber-attacks.[57] It is important to note that this risk is unique to cloud computing and that this service engine does not exist in standard IT infrastructure.

Management Interface Platform Compromise: Unique

Clients access their cloud computing resources through a management interface. This is the client-facing platform that allows clients to interact with their CSP and describe their computing needs, as well as interface with their virtual machines. Every CSP has a unique platform where clients login to the system, but clients of the same CSP share a common management interface. As with any software, it can be prone to bugs that can be leveraged to abuse the system and gain unintended privileges. According to interviews

[56] RedLock CSI Team. "The Cryptojacking Epidemic." February 2018.
[57] Securing Cloud Computing Systems pg 100.

with network security specialists, a compromised platform could allow malicious actors could access information of other clients. Clients must also understand how to properly configure the controls on the interface as misconfigured controls could unintentionally expose the firm to additional risk through data exposure or unauthorized access.

Encryption Key Storage: Escalated (increase probability)

Encryption key storage is a basic and important principle in managing security best practices as theft or misuse of these keys could result in sensitive data being exposed. Encryption provides a strong and reliable method of protecting information, but it is the handling of those encryption keys that poses a weak point. Because these keys are stored on the CSP network, it is essential to ensure that they are properly protected and that access to key stores is limited by separating roles to control access. Additionally, if the private key, the tool used to decrypt information, is lost then the encrypted data will no longer be accessible.

General Risks

Natural Disaster: Escalated (increase probability, decrease impact)

Although the risk generated from natural disasters is not unique, it is escalated through the use of cloud computing as the CSPs' servers are spread out in multiple locations and therefore they are subject to a greater variety of environmental effects. Despite the increase in probability, business continuity becomes more resilient as CSPs can port functions by leveraging servers in other data centers.

Social Engineering: Escalated (increase probability)

Social engineering is one of the most common and prolific cyber risks that threaten enterprises today. The risk is typically managed through educating "good cyber hygiene"; however, as banks adopt cloud services, they cede control over certain parts of the operation and lose visibility on phishing schemes targeted towards CSPs.

Contractual Risk: Escalated (increase probability, increase impact)

As with any outsourcing of operations, the relationship between the client and service provider is generally outlined and defined in a legal document, raising the issue of legal risk. In the case of CSPs and their clients, the terms of the relationship are provided through private contract called a Service Level Agreement (SLA). The risk here occurs from a failure of banks to clearly delineate responsibilities and controls of the CSPs as well as the client's abilities to enforce actions in the case of breach of contracts.

Interdependencies: Escalated (increase impact)

Interdependencies cover the entire infrastructure on which CSPs rely to conduct their business, such as the internet. This also includes electricity generation and cables that transfer data from the cloud to the client. Similar to the issue of natural disaster, as the infrastructure becomes more diffuse, the surface space for disruption also increases. Moreover, access to the cloud is generally dependent on connectivity to the internet and this is will be even more salient with the proliferation of the Internet of Things.

Risk Mitigation Techniques and Procedures

As major financial institutions move more functions to the cloud, the more integral cloud providers will become to the financial system. Even if CSPs do not rise to the level of critical infrastructure, their connection to the financial industry creates risk through cyber transmission channels. "From a cyber perspective, the small-value/volume participant or a vendor providing non-critical services may be as risky as a major participant or a critical service provider."[58] Based on our interviews, banks are keenly aware of this issue and the majority of banks thus far have abstained from outsourcing core functions to the cloud to mitigate the impact of this risk. However, this is not completely ubiquitous. Since 2015, Capital One began experimenting moving critical operations to AWS.[59] Therefore, it is important to note that this environment is changing and banks will likely test out new ways to structure their operations to increase efficiency and reduce costs.

However due to the nature of cyber transmission channels and the highly interconnectedness of the financial industry, keeping core functions off of CSP networks will not in itself remove the risk to financial stability. Technology plays a pervasive role in gathering information, conducting analysis, and executing functions within the financial system and any lapse in IT security has the potential to be leveraged to create a channel to access other IT systems, some of which could be critical in sensitive financial transactions. To be sure, this risk can be managed through risk avoidance, risk reduction, and risk transfer techniques[60], but it cannot be eliminated. Financial firms must determine how to balance their business and risk decisions so that they operate within their risk profile.

In the context of cybersecurity and cloud computing, banks have been active in employing a mix of management tools and technical solutions to mitigate risk. According to our interview with industry experts, G-SIBs have applied multi-cloud architecture models for mission critical operations. This includes maintaining a full stack on both their public and private clouds at all times as well as geo load balancing[61] and utilizing technologies at the network level to dynamically switch between services. Large organizations like G-SIBs also deliberately spread out their infrastructure so that servers are not all concentrated in the same geographical location, a principle that is ensured through their contractual agreements with CSPs. G-SIBs are very active in mitigating risk to their business operations and are increasingly monitoring systemic financial stability. It is in this regard that it is essential that regulators understand the risks banks face when using CSPs, their techniques for managing this risk, and how, if any of these strategies create vulnerabilities in the system as a whole.

[58] CPMI IOSCO 2016 guidance.
[59] AWS. "Capital One Case Study." January 2018.
[60] IMF Working Paper. "Cyber Risk, Market Failures, and Financial Stability." August 2017.
[61] Moving traffic between multiple data centers in different locations.

Source: Zurich Insurance Company. "Beyond Data Breaches: Global Interconnections of Cyber Risk". April 2014.

Risk Mitigation for the Cloud

Many of the risks listed above can be mitigated through cloud consumers' attention to vendor risk management tailored to address the nuances of the cloud. General vendor risk management is defined as the "process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance."[62] We identified four key non-regulatory ways for cloud consumers to tailor existing frameworks to mitigate risk in their cloud adoption practice: 1) Service Level Agreements (SLAs), 2) Auditing certifications and standards with a focus on Service Organization Controls (SOC), 3) The National Institute for Standards and Technology (NIST) Management Framework for Cloud Ecosystem (RMF4CE), and 4) Cyber insurance.

Service Level Agreements

SLAs are foundational for risk mitigation in the event that something goes wrong with the cloud. SLAs between cloud consumers in the financial services industry and CSPs are fundamentally a contract that set expectations for the relationship.[63] They are widely recognized as a useful tool that ultimately sets parameters related to the stability of the cloud service, protects the assets of the company using the cloud, and minimizes expenses in the event of cloud disruption or failure. [64] Regulators also view SLAs as an

[62] Gartner. "Vendor Risk Management." 2017.https://www.gartner.com/it-glossary/vendor-risk-management.
[63] Wired. "Service Level Agreements in the Cloud."
[64] Ibid.

important tool for risk mitigation. This is evidenced by the European Banking Authority's (EBA) recent prescription of terms related to data security in the cloud to be included in the SLAs.[65]

At this time, the maturity and standardization of SLAs for cloud computing are evolving. This leaves room for misinterpretation of terminology by both cloud consumers and CSPs which can result in a decline of usability of the SLA.[66] While improvements to standardization have been made throughout the past several years given that cloud consumers are better educated regarding risks associated with cloud adoption, it is still important for cloud consumers to carefully define parameters.[67] These include defining parameters such as performance as well as how CSPs measure that provision of service.[68] Another common issue is a lack of reassessing the SLA as services are either added or amended by either party. The SLA is a living document that serves as a roadmap should changes occur within the cloud – as such, reassessment is necessary.[69] Thus, it is critical for banks to ensure clear delineation of responsibilities and controls within their SLAs so they can better evaluate the components of their risk management.

From our interviews, we heard that banks who first adopted CSPs have had first-mover advantage, meaning the bank could make requests for greater transparency and control over various factors included in the SLA. However, it appears that this will not be the trend moving forward, particularly for small to medium sized firms and even for larger institutions that are late adopters as their leverage in this area will diminish in the future.

Auditing the Cloud

The widespread adoption of cloud computing raises questions regarding whether current auditing certifications and standards conducted by third-parties are sufficient to provide a clear picture risk assessment for the cloud. This is pertinent to the financial services industry because firms evaluate business risks associated with cloud utilization strategies alongside the evolution of cloud technology. Challenges for cloud consumers include ensuring that members of the financial services industry and auditors understand and examine the following: 1) the scope of the cloud computing environment, 2) risk assessment standards to analyze risks accurately, and 3) audit trails.[70]

Generally, both auditors and compliance teams have considered audit challenges posed by cloud for over a decade, allowing for current standards to mature alongside the technology. Useful tools and frameworks utilized by both members of the financial services sector and auditors include NIST SP 800-53, 144, 30, ISACA's Cloud Computing Audit Program, Cloud Security Alliance – Cloud Controls Matrix, and the Federal Risk and Authorization Management Program.[71]

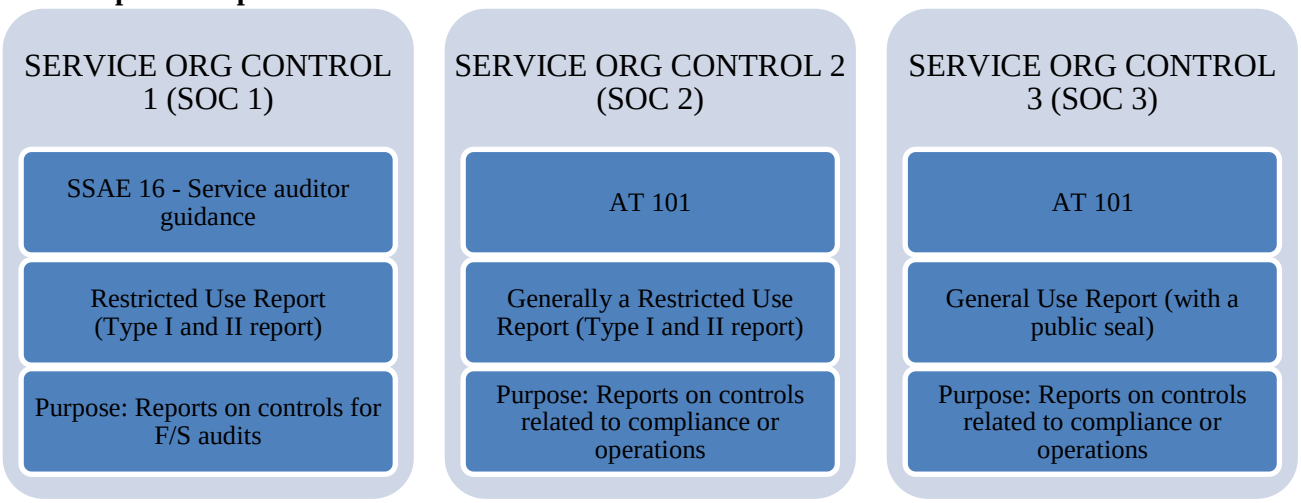
---

[65] Rathod, L. "European Banking Authority: New Outsourcing Guidelines Seek to Clear the Path to the Cloud for the Finance Industry." Diligent. 2018.; EBA. "Recommendations on Outsourcing to Cloud Service Providers." 2017.
[66] SANS. "Proposal for standard Cloud Computing Security SLAs – Key Metrics for Safeguarding Confidential Data in the Cloud." 2015.
[67] Cloud Technology Partners. "How to Slay the Dragon of Cloud SLAs." 2017; IBM. "Best Practices to Develop SLAs for Cloud Computing." 2013.
[68] Ibid; Michael Cooney. "10 Best Cloud SLA Practices." Network World. 2016.
[69] Walayat Hussain, Omar Hussain, Farookh Hussain, "Maintaining Trust in Cloud Computing Through SLA Monitering." 2014; Wired. "Service Level Agreements in the Cloud."
[70] Deloitte. "Cloud Computing – What Auditors Need to Know." 2014.
[71] Ibid.

Service and Organization Controls (SOC)

In conjunction with frameworks utilized by cloud consumers and third-party auditors listed above, SOC 1, 2, and 3 Reports generated by independent third-party auditors serve as a valuable resource and a baseline for risk managers in the financial services industry. SOC 1 articulates controls over financial reporting of CSPs, whereas SOC 2 and 3 cover safeguarding data and information by examining controls over non-financial reporting.[72] SOC 2 certifications are the most helpful for cloud consumers given that they verify that a cloud provider is able to effectively implement their services.[73] The report also provides transparency regarding the nature of controls implemented by cloud service provider as well as the tests that auditors perform.[74]

SOC Report Comparison



Source: AIPCA. "Explaining SOC." June 2012.

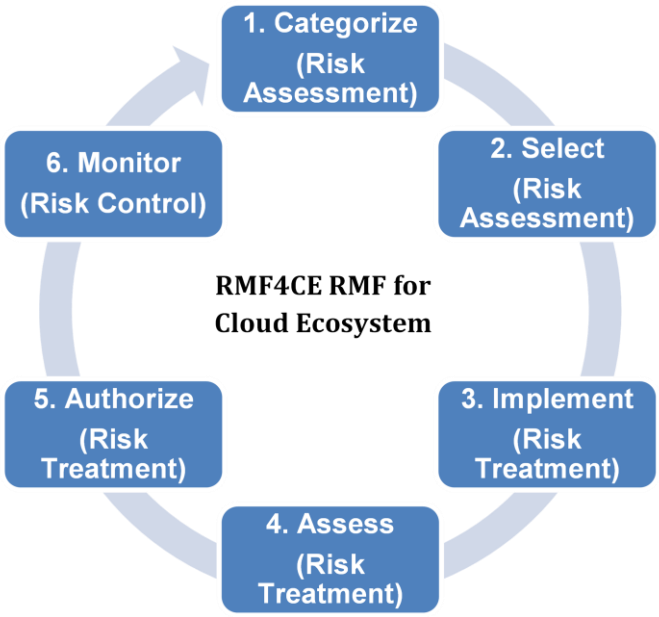
According to auditing firms that we interviewed, the SOC 2 report is the basis for any third-party outsourcing that needs to consider cybersecurity. One of the primary challenges related to SOC 2 reports in the context of CSPs is that the reports are too generic in nature. Many of the reports provide an overview of the broad environment surrounding assurances and risk management for all clients on the CSP but do not account for special requirements or controls that relate to specific industries such as financial services. This leads members of the financial services industry to question whether their individual infrastructure is being managed properly and to request increased transparency. According to experts, because of the size of the market as well as regulatory environment, CSPs have allowed teams to observe and inspect security controls, but this may not be the norm going forward.

NIST Framework for the Cloud Ecosystem

[72] PWC. "System and Organization Controls Reporting."
[73] Bluelock. "3 Things to Know About SOC 2 Compliance and Cloud Providers." 2018.
[74] I.S. Partners. "SOC 1 and SOC 2 Reports – Do you Know the Difference?" 2018.

The U.S. Federal Chief Information Officer tasked NIST with assisting the federal government to adopt the cloud in 2010.[75] Since that time, members of the NIST staff have established themselves as experts in the space and provide guidance to members of the public and private sectors.

NIST's RMF4CE, published in 2015, is a helpful tool that tailors NIST's traditional RMF to the cloud ecosystem.[76] The framework can be used by cloud consumers to mitigate security risks that stem from cloud based information systems. By helping cloud consumers map out risks associated with cloud adoption, it better allows them to incorporate specific risks into the terms and conditions in the contracts, such as SLAs, with external providers and brokers.[77]



Source: NIST – Risk Management Framework. "Managing Risk in the Cloud". 2015.

Cyber Insurance Overview

Executives in the financial services industry agree that cyber insurance will continue to play an increasing role in financial risk-mitigation strategies and resilience planning. Cyber insurance policies drive behavioral change through creating positive incentives – even the act of applying for cyber insurance prompts firms to think through their cybersecurity frameworks.[78] Insurers are further incentivized to help clients avoid cyber attacks and may even offer services such as monitoring and incident response support to clients.[79] Given the many benefits associated with cyber insurance, the industry annual gross premiums are expected to increase to approximately $7.5 billion by 2020.[80]

Cyber Insurance and Vendor Risk Management

While the cyber insurance industry continues to grow, and evolve, cyber policies are not a panacea for risk-mitigation. The cyber insurance market is underdeveloped and lacks standardized policies, especially related to policies related to cloud computing. This is because underwriters lack data to adequately price

[75] NIST. "NIST Publishes Draft Cloud Computing Security Document for Comment." 2013.
[76] NIST. "Managing Risk in a Cloud Ecosystem"; Iorga, M. "Managing Risk in a Cloud Ecosystem." "IEEE Cloud Computing, vol. 2, no. 6, pp. 51-57, Nov.-Dec. 2015.
[77] Ibid.
[78] Marsh and McLennan. "The Role of Cybersecurity in Risk Management." 2016.
[79] Marsh and McLennan. "The Role of Cybersecurity in Risk Management." 2016.
[80] PwC. "Insurance 2020 and beyond: Reaping the dividends of cyber resilience." 2015.

financial losses caused by cyber events – a problem that is compounded by the rapid evolution of threats.[81] Insurers compensate for this lack of data and concentrated cyber risk by charging more for policies. To cap loss potential, policies also contain extensive restrictive limits, exclusions, and conditions.[82]

Currently, the majority of policies related to third-party vendors cover the following events: 1) breaches related to employee confidentiality, 2) lost client information and data, 3) notifying clients after a security breach, and 4) efforts related to public-relations, defamation, and intellectual property violations.[83] This does not include loss of revenue due to interrupted business operations – a scenario that could easily occur if banks place key revenue generating businesses into the cloud that face significant losses in the event of an outage.[84]

As increased adoption of both cloud computing and the purchase of cyber insurance policies occur, firms should carefully examine and map out their use of technology and review third-party vendors. According to experts, for the foreseeable future it is unlikely that current insurance products will provide adequate coverage in the context of cloud computing for the financial services industry. Mapping out the risks, particularly as they relate to concentration on the cloud, is an important next step for firms to receive broader coverage.

Observations & Analysis

- Outsourcing computing capabilities to CSPs decreases risk for network security but increases operational risk.
- Additional controls & considerations need to be implemented into IT network & governance protocols, focusing on escalated or unique risks.
- Concentration risk in relation to CSPs exists at two distinct levels: the firm level and industry level.
    - At the firm level, banks must consider both using multiple CSPs as well as specifying their desire to diversify compute capabilities among multiple servers in different locations
    - At the industry level, G-SIBs should not all reside on the same CSP or rely on the same cloud servers
- Third-party audit practices such as SOC 2 are generally evolving to account for the nuances of cloud computing.
- CSPs provide extensive support to members of the financial services industry as they work to map out risks associated with cloud adoption. As an example, AWS published one of the first compliance workbooks specifically designed to assist financial institutions navigate FFIEC audits and compliance for AWS.
- At this time, SLAs lack standardization related to key parameters such as performance in the context of cloud computing. This can pose significant problems for members of the financial services industry as well as CSPs if sufficient care is not taken to standardize terms and definitions.

[81] Ibid.
[82] Ibid.
[83] The Data Center Journal. "Ten Things You Need to Know about Cybersecurity Insurance."
[84] Woodruff, Sawyer, and Company. "Cyber Insurance 101: Cloud Computing and Liability."

Part 3: The Role of Regulators & the Future of Cloud, Finance, and Government

Financial regulation is designed to reduce systemic risk and foster financial stability. Around the world, financial regulators have begun drafting cyber-specific (and in some jurisdictions, cloud-specific) rulemaking to address the ever-evolving role that technology plays in the financial sector. According to the G-20 Financial Stability Board (FSB), regulators have consistently looked to a few pre-existing bodies of guidance and standards to develop their own regulatory and supervisory schemes.[85] The most commonly referenced standards are:

- Guidance on Cyber Resilience for Financial Market Infrastructures (or CPMI-IOSCO Guidance) by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO)
- Framework for Improving Critical Infrastructure Cybersecurity (or NIST Cybersecurity Framework) by the US National Institute of Standards and Technology (NIST)
- The International Organization for Standardization 27000 Series (or ISO 27000 Series)[86]

Most cybersecurity frameworks are silent on cloud risk. Cloud risk is assumed to be addressed as third-party vendor risk and is no different from risks posed by other technology service providers. In the U.S., this approach brings CSPs under the jurisdiction of US banking authorities, allowing any CSP activity performed for a bank to be monitored as closely as if it were managed by the bank itself[87]. However, the way in which these frameworks assess cloud risk also ignores some of the unique risks posed by cloud adoption, such as concentration risk. In order to address systemic risk, regulators must also consider the possibility that CSPs are becoming critical to the function of the financial system and may require differentiated guidance and supervision than other third-party vendors.

Influential Frameworks

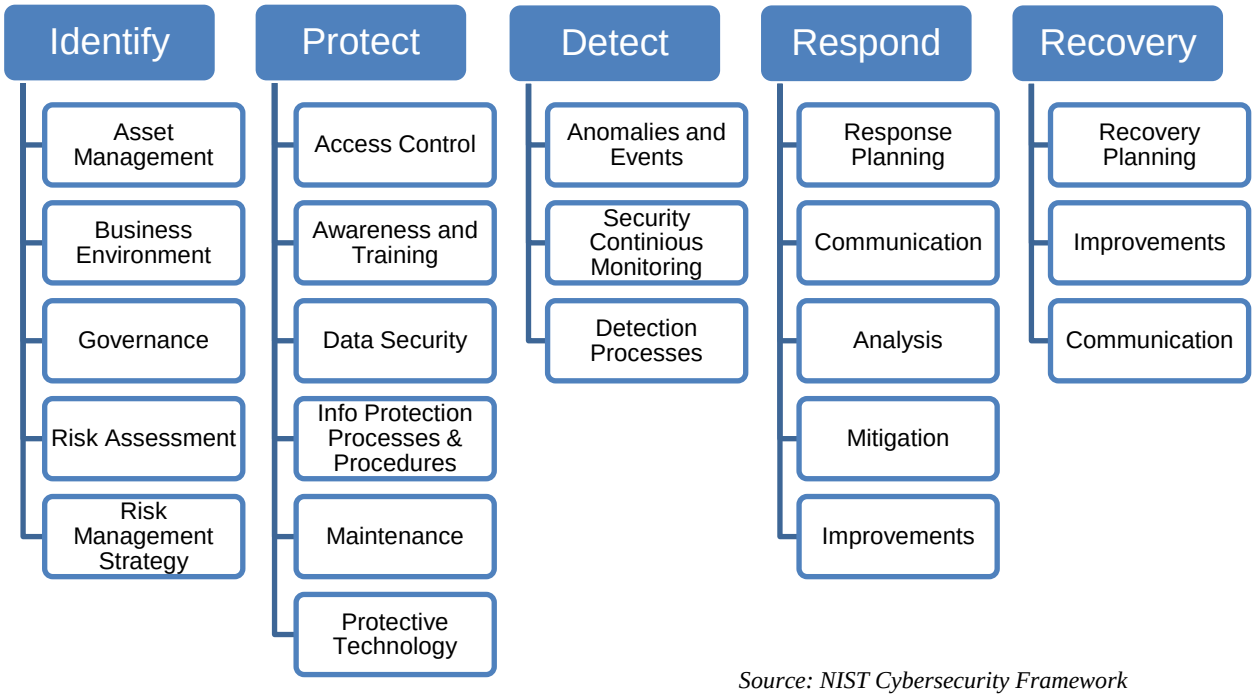
NIST Cybersecurity Framework: 2014

In 2014 NIST published the Cybersecurity Framework, which has become the most widely adopted cybersecurity framework among financial institutions and regulatory bodies. The Framework was a collaborative effort between NIST and the private sector that uses existing industry standards and best practices to help organizations manage their cybersecurity risk.

[85] FSB. "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices." October 2017.
[86] Ibid.
[87] FDIC. "Bank Services Company Act." 1999.

The NIST Framework Core provides a set of actions an organization can undertake for cybersecurity outcomes. It is important to note that the Core is not a prescriptive checklist; rather, it provides key

NIST Framework Core



Source: NIST Cybersecurity Framework

cybersecurity outcomes that have been identified by industry experts as useful for mitigating cybersecurity risk.[88] At the highest level, the Core consists of five basic cybersecurity functions: Identify, Protect, Detect, Respond, Recover (Exhibit x). Ultimately, the Core provides financial institutions with a roadmap to either establish a cybersecurity program or review and improve on an existing program.

Although the original NIST Framework offered no specific recommendations for assessing cybersecurity risk related to cloud adoption, NIST has released a number of cloud-related guidance, such as the 2011 "Guidelines on Security and Privacy in Public Cloud Computing", that are intended to be used in coordination with the Framework. Recently, NIST published an update of the original framework, NIST Framework 1.1 to incorporate supply chain risk management. During the comments period, more than 70 organizations and individuals commented on the update including The Financial Services Sector Coordinating Council (FSSCC) which "largely supported" the changes to the framework.[89] FSSCC expects that the NIST Framework with the "development of a risk-tiering methodology specific to the financial services sector" would be "more widely adopted by financial sector institution and government agencies."[90]

[88] NIST. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0." February 2014.
[89] Ibid.
[90] Ibid.

ISO 27000 Series: 2013

ISO 27000 is a series of information security standards published in coordination with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The 27000 series specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of an organization.[91] The ISO27k core documents are 27001 and 27002 which specify the requirements for ISMS and establish guidelines for implementation. The standards utilize a Plan-Do-Check-Act model for continuous quality control and improvement, which is highlighted in the 6-part planning process:

1) Define a security policy
2) Define the scope of the ISMS
3) Conduct a risk assessment
4) Manage identified risks
5) Select control objectives and controls to be implemented, and
6) Prepare a statement of applicability[92]

The key advantage to ISO27k and the reason for its success is its alignment with business objectives, since the goal of the series is to ensure data security while maximizing operational efficiency.

In 2015, ISO released a document supplementing the guidance of the 27002 standard that contains specific language pertaining to both cloud service clients and CSPs, with primary guidance laid out side-by-side in each section (Exhibit x). This standard is not intended to be a comprehensive guide to cloud adoption, but rather a starting point for organizations who wish to implement cloud computing in a way that is compliant with existing ISO standards. The standard focuses heavily on establishing clear agreements between cloud service clients and providers, solidifying the importance of robust service level agreements as a risk mitigant. ISO also stated that it has no plans to certify the security of CSPs specifically, judging that it is sufficient to certify them compliant with ISO/IEC 27001 like any other organization.[93]

[91] ISO. "ISO/IEC 27001:2013." October 2013.
[92] Pelnekar, C."Planning for and Implementing ISO 27001." ISACA Journal (4). 2011.
[93] IsecT. "ISO/IEC 27017:2015/ ITU-T X.1631 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services." 2018.

ISO/IEC 27013:2015 Cloud-Specific Information Security Controls	
Cloud Service Client	**Cloud Service Provider**
"The cloud service client should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement. The cloud service client should identify and manage its relationship with the client support and care function of the cloud service provider."	"The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service clients, its cloud service providers, and its suppliers."

Source: see ISO 27017:2015

CPMI-IOSCO Guidance

In 2016, CPMI and IOSCO released guidance on cyber resilience for financial market infrastructures (FMIs). The guidance is significant because it was the first set of internationally agreed upon principles for financial markets and institutions to support consistent and effective oversight in the area of cyber resiliency.[94]Additionally, because the guidance is technology-neutral, it can easily be expanded to cover new types of third-party vendor risk, such as cloud adoption, without significant rewrites. This type of structure is important for all banking supervisors looking to regulate the cloud.

There has been some criticism of the guidance, specifically with regard to the section that implemented a recovery time objective (RTO) which recommended that a FMI be able to resume critical operations within two hours of a cyber event, and complete settlements by the end of the day. The 2-hour RTO was seen as overly-prescriptive by some stakeholders, and most expressed the view that the objective would not be feasible or practical in all scenarios.[95]

US Regulation and Guidance for Financial Institutions

US regulatory bodies have looked to these three resources (NIST, ISO, CPMI-IOSCO) for inspiration when drafting guidance for cybersecurity. Currently, there are no US financial regulations specifically aimed at cloud adoption by financial institutions or the operation risk inherent in this practice. There are also no regulations that create binding minimum obligations for financial institutions when it comes to managing any type of cyber risk. US regulators have written guidance aimed at managing third-party risk and managing cyber risk with the intention of it applying to the cloud, yet most of the guidance fails to explicitly deal with the risk of outsourcing to CSPs.

Third Party Risk

OCC Bulletin 2013-29: Released in 2013, the OCC risk management guidance for third-party relationships emphasizes a top-down, technology-neutral approach to risk assessment. The bulletin expanded the OCC's

[94] ECB. "Cyber Resilience for Financial Market Infrastructure." January 2016.
[95] See "Comments received on 'CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures – consultative paper." 2016.

previous definition of third-party relationships to include "any business arrangement between a bank and another entity, by contract or otherwise."[96] This broadened definition allows the vast majority of third-party relationships to fall under OCC supervision. Under the new bulletin, risk assessment is extended to include fourth-party risk and introduces the idea of "critical activities" and expects that banks will use a more rigorous process to evaluate third-party vendor risk relating to these activities. These critical activities include bank functions such as payments, clearing, settlements and custody, and shared services such as information technology. Lastly, the bulletin states that "a bank should adopt risk measurement processes commensurate with the level of risk and complexity of its third-party relationships," indicating that the OCC's approach to evaluating third-party risk will be risk-and principles-based, rather than prescriptive.

As written, the OCC Guidance covers CSPs as third-party vendors, so it is unclear if the OCC will introduce additional guidance for financial institutions and cloud adoption. In 2017, the OCC released Supplemental Examination Procedures to the original bulletin, but continued to maintain a technology-neutral approach, suggesting that cloud-specific guidance is not an immediate priority.

The OCC does have the ability to examine a bank's vendors under the Bank Service Company Act (12 U.S.C. 1867) which grants federal banking agencies the authority to examine and regulate the activities of third-party service providers to the same extent as if these were performed by the bank itself. Our interviews have revealed that US bank supervisors are not currently exercising their authority when it comes to CSP examination; however, the regulators are fostering a direct relationship with the CSPs and are relying on SLA agreements to prove that banks are appropriately managing their vendor risk.

Cybersecurity

Bank Supervision Operating Plan for Fiscal Year 2018 (OCC): Released in September 2017, this year's OCC's operating plan included measures specifically for cybersecurity and operational resiliency. The plan suggests that agency examiners review bank's information security programs to assess the cyber threat environment and a bank's cyber resilience.[97] The plan also includes provisions for the Chief National Bank Examiner (CNBE), in coordination with other supervisory agencies, to conduct examinations of service providers (including CSPs) with a focus on cybersecurity and resilience, enterprise risk management, interconnectivity, and third-party risk and compliance risk management. The operating plan importantly extends the reach of financial oversight agencies to examine CSPs, and incorporates reviews of cloud computing for critical services in financial institutions. Examiners are instructed to assess management structures and cyber resilience of technology service providers (TSPs) by completing the FFIEC's TSP Cybersecurity Assessment Tool.

The 2017 Cybersecurity Assessment Tool (FFIEC) is irrefutably the most widely used examination method for both regulators and financial institutions. The assessment was first published in 2014 and its content and methodology are consistent with the FFIEC IT Examination Handbook, the NIST Cybersecurity Framework, and accepted industry best practices such as the ISO 27000 series. The assessment is divided

[96] OCC. "Third-Party Relationships: Risk Management Guidance." 2013.
[97] OCC. "Fiscal Year 2018 Bank Supervision Operating Plan." September 2017.

into two parts: 1) Inherent Risk Profile, which identifies the institution's inherent risk level; and 2) Cybersecurity Maturity, which measures the sophistication of a firm's controls and practices.[98] Once both components are completed, financial institutions are expected to review the relationship between Inherent Risk Profile and domain Maturity Levels. While a certain Maturity Level is not required of an institution, a misalignment between risk profile and maturity should be remediated by management.[99]

The assessment considers cloud adoption in the Inherent Risk Profile. Institutions are asked to estimate their risk level based on their use of cloud computing services to support critical activities. Interestingly, the assessment considers using a substantial number of cloud providers, public cloud and internationally located clouds to be the "most" risky behavior. The risk of diversification of CSPs would seem counterintuitive to the financial stability concern of concentration risk with regard to the cloud adoption.

FFIEC Risk Assessment of Cloud Adoption

Category: Technologies and Connection Type	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Cloud Computing services hosted externally to support critical activities	No cloud providers	Few cloud providers; private cloud only (1-3)	Several cloud providers (4-7)	Significant number of cloud providers (8-10); cloud- provider locations used include international; use of public cloud	Substantial number of cloud providers (>10); cloud-provider locations used include international; use of public cloud

Source: FFIEC Cybersecurity Assessment Tool

2016 ANPR Enhanced Cyber Risk Management Standards FRB, OCC, FDIC): In 2016, the FRB collaborated with the OCC and FDIC to issue a joint advance notice of proposed rulemaking (ANPR) with regard to cyber risk management. It is the only proposed regulation aimed specifically at cyber risk associated with financial institutions and their service providers. Unlike NIST and the FFIEC Cybersecurity Assessment Tool, the ANPR would establish binding minimum standards for the largest and most interconnected US financial entities. The agencies also considered applying the standards to third-party service providers to ensure consistent, direct application of standards. The proposed standards were organized into five categories:

1) Cyber risk governance
2) Cyber risk management
3) Internal dependency management
4) External dependency management and
5) Incident response, cyber resilience, and situational awareness.

[98] FFIEC. "Cybersecurity Assessment Tool." May 2017.
[99] Ibid.

Standards would be divided into two tiers, with the most stringent standards applying to systems of institutions that are deemed systemically important, and less stringent rulemaking applied to smaller, less interconnected institutions.[100] The standards included the concept of "sector-critical systems", which are covered entities that are critical to the functioning of the financial system. These systems are not explicitly defined, leaving open the possibility that CSPs could be identified as sector-critical systems due to their size and interconnectedness. The ANPR would be more rigorous than previous guidance, with a primary goal of protecting the financial system, rather than institutions.

The Clearing House Responds

In February, 2017, the Clearing House Association responded to the agencies' invitation to comment on the ANPR, issuing a lengthy critique of the proposed standards. Among the Association's recommendations were:

- **Scope:** The ANPR's $50 billion asset cutoff should be replaced with a multi-factor risk-based standard
- **Service Provider Requirements:** These requirements should be implemented through the service provider's oversight agency rather than adding additional vendor oversight for financial institutions
- **Cyber Risk and Governance:** Financial institutions should have discretion to determine how to structure supervision of their cyber risk management
- **Cyber Risk Management:** Financial institutions should have flexibility in developing their risk management strategy
- **Internal and External Dependency Management:** The enhanced standards should be limited to business assets that are most likely to raise material risks to the financial institution's cybersecurity and on third-parties with access to key systems
- **Incident Response, Cyber Resilience and Situational Awareness:** Standards should be risk-, rather than outcome-focused
- **Sector Critical Systems:** The scope of sector-critical systems should be narrow, predictable and focused

Source: The Clearing House. "Re: Enhanced Cyber Risk Management Standards." February, 2017

The ANPR has not been advanced to become a binding regulation and it was generally criticized by members of the financial industry and by independent consultants for being overly prescriptive and needlessly increasing the burden of regulation on the industry. In particular, critics targeted the RTO that would be mandated by the standards, citing the two-hour standard as either costly or not feasible.[101] The ANPR has not been advanced for further consideration.

Current Industry Best Practices

Financial institutions and regulatory bodies have historically coordinated with each other generating a series of industry best practices to improve cyber resiliency of the financial system. These practices include cyber exercises, data backup solutions, and information sharing platforms which should be evaluated to see how they could apply more appropriately to cloud adoption.

[100] OCC, FRB & FDIC. "Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards." October 2016
[101] Covington & Burling, LLP. "Federal Banking Agencies Request Comment on Enhanced Cybersecurity Standards." October 2016.

Cyber Exercises

Current cyber exercises in the US, such as Hamilton Series and Quantum Dawn Series, are essential to the promotion of financial stability against cyber threats. These exercises have been helpful in addressing cybersecurity issues by testing for vulnerabilities in IT infrastructures and providing resolution strategies for the financial industry, regulators, and government stakeholders.

The Hamilton Series of exercises were developed in collaboration with the FSSCC, the FS-ISAC, the US Treasury Department and other US government agencies. These exercises prepare bank supervisors and financial sector participants for cyber-attacks by simulating various attacks or incidences.[102] Lessons from the series have helped the public and private sector improve their policies, procedures, and response capabilities, which has helped increase the cyber resiliency of the financial industry.[103]

Quantum Dawn is a biennial series of market-wide simulations utilizing service provider Norwich University Applied Research Institutes (NUARI) to better prepare the financial industry and their public partners for crisis response to cybersecurity issues. [104] For example, held in November 2017, Quantum Dawn 4, a "closed loop" simulation with participants from financial institutions and government agencies, was a distributed exercise exploring a disruption to futures activity and the knock-on effects to the cash market. It "[aimed] at improving the readiness of individual financial institutions to coordinate as a sector and with key government partners to respond to and recover from a systemic cyber event."[105] Lessons from the Quantum Dawn series highlighted the importance of public-private partnership in information and intelligence sharing and the significance of collaboration in protecting the market from cyber threats.

Sheltered Harbor was instituted as a result of the Hamilton Series and is a voluntary, industry-led initiative created by the US financial industry to enhance the business continuity and disaster recovery strategies of the financial sector. Members of the Sheltered Harbor convert their data to a "Sheltered Harbor industry-standard format" on a daily basis, apply standard strong encryption to data, and transfer the data to a vault.[106] If client data is compromised or deleted in a cyber event that disrupts critical processing capability or has implications for consumer confidence, member institutions can retrieve and decrypt their data from the vault and continue operating.

While these exercises and backup solutions are beneficial in mitigating the impact of cyber events and promoting financial stability, they have not, to date, paid significant attention to cloud-related incidents. As the financial industry becomes more dependent on the cloud, cloud-based third-party vendor risks should be more adequately incorporated into future exercises and initiatives.

Information Sharing Programs and Collaborative Industry and Governmental Bodies

Information sharing of cyber event indicators, cyber and physical threat intelligence, analysis, and possible response strategies, is essential to promoting cyber resiliency among the financial sector. Existing

[102] FS-ISAC Exercises. "The Hamilton Series." 2018.
[103] FSSCC. "Financial Services Sector Cybersecurity Recommendations." January 2017.
[104] Deloitte, SIFMA. "Standing together for financial industry cyber resilience Quantum Dawn 3 after-action report." November 2015.
[105] SIFMA. "Fact Sheet: Quantum Dawn IV." November 2017.
[106] Sheltered Harbor "How it Works". 2018.

information sharing platforms play an essential role in helping the financial system tackle cyber-related issues, including cloud outages and breaches. There are two major information sharing platforms established by the financial sector the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Financial Systemic Analysis & Resilience Center (FSARC). Additionally, there are two major collaborative industry and governmental bodies that address cybersecurity issues, the Financial Services Sector Coordinating Council (FSSCC) and the Financial and Banking Information Infrastructure Committee (FBIIC).

Financial Sector Information Sharing Programs

Name	Public/Private Sector	Main Function	Members	Main Objectives
FS-ISAC[107]	Private Sector	Information sharing platform	• Financial service industry	• Cyber and physical threat intelligence • Timely, relevant, and actionable incident information • Alerts, analysis, best practices and other critical information
FSARC[108]	Private Sector	Information sharing platform	• Large financial institutions identified as critical infrastructure	• Current and emerging cybersecurity threats posing a systemic risk to the financial system
FSSCC[109]	Private Sector	Collaborative body	• Financial trade associations • Financial utilities • Critical financial firms	• Cybersecurity issues of all types • Natural disaster readiness
FBIIC[110]	Public Sector	Collaborative body	• Financial regulatory community (both federal and state)	• Operational and tactical issues related to critical infrastructure matters, including cybersecurity, within the financial services industry

Interviews with financial industry and regulation experts confirmed the importance of information sharing platforms, however, there were differing opinions on how they should be used. From the government/regulators' perspective, financial institutions are still too hesitant to share sensitive information. Although some of the liabilities for sharing confidential information were removed by the Department of Justice[111], financial institutions continue to struggle because they are responsible for making

[107] FS-ISAC. "Sharing Critical, Authoritative Information Across our Industry." 2018.
[108] FS-ISAC. "FS-ISAC announces the formation of the Financial Systemic Analysis & Resilience Center (FSARC)." October 2016.
[109] FSSCC. "Protecting Critical Infrastructure". 2018.
[110] FBIIC. "Mission & History". 2018.
[111] Harvard. "Cybersecurity Information Sharing Act." December 2015.

the decision of what to share, how to share, and who to share with based on their own assessment of materiality. With the improvement of information sharing channels, financial institutions could more easily share updated and relevant information with regulatory bodies. This could also allow the public sector to coordinate with financial institutions to reduce the gaps and overlaps of current regulations and decrease the regulatory burden and compliance costs to the private sector.

Comparisons to Other Jurisdictions

Regulators are recognizing the global trend of cloud adoption among financial institutions and have responded accordingly in some regions with regulations and recommendations. Hong Kong, Singapore, United Kingdom, and the European Union are prime examples of jurisdictions that have produced regulations, guidance, and recommendations on cloud adoption for financial institutions. These frameworks could act as foundations to building US regulatory and supervisory practices relating to cloud adoption of the financial industry.

Hong Kong and Singapore's monetary authorities both support and promote cloud adoption by banks and have produced sophisticated outsourcing guidelines to address cloud adoption by financial institutions.[112][113] In Hong Kong, authorized institutions are required to perform risk assessments and due diligence reviews of CSPs, to make sure controls are in place to protect data confidentiality and establish contingency arrangements.[114] In Singapore, financial institutions do not require prior approval or notification of outsourcing arrangements[115] but should "be ready to demonstrate how they are compliant". Additionally, the Monetary Authority of Singapore also notes that "the types of risks of cloud services (CS) are not distinct from that of other forms of outsourcing arrangements."[116] Since 2003, The Hong Kong Monetary Authority has recognized the concentration risk associated with outsourcing and in their General Principles for Technology Risk Management they recommend that "authorized institutions should try to avoid placing excessive reliance on a single outside service provider in providing critical technology services."[117] Singapore was more rigorous in producing cloud adoption guidance and in 2016, the Association of Banks in Singapore (ABS) released the Cloud Implementation Guide 1.1 (ABS Guide) which is the first cloud implementation guide that specifically applies to banks. It provides banks with different cloud deployment models, helps banks to determine "material" and "non-material" outsourcing and recommends a set of due diligence and vendor management activities for CSPs that banks can consider.[118] Additionally, the Singapore Standard Council published the Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584 in 2016, which is "the world's first cloud security standard that covers multiple tiers of cloud security."[119]

[112] John Kang, Ranajit Dam. "Journey to the Cloud." June 2017.
[113] AWS. "AWS User Guide to Financial Services Regulations & Guidelines in Hong Kong." November 2017.
[114] AWS. "AWS User Guide to Financial Services Regulations & Guidelines in Hong Kong." November 2017.
[115] Microsoft. "Navigating your way to the cloud – Microsoft's response to the MAS Outsourcing Guidelines and the ABS Cloud Implementation Guide." November 2016.
[116] Monetary Authority of Singapore. "Guidelines on Outsourcing." July 2016.
[117] Hong Kong Monetary Authority. "Supervisory Policy Memo TM-G-1: General Principles for Technology Risk Management." June 2003.
[118] The Association of Banks in Singapore. "ABS Cloud Computing Implementation Guide 1.1." August 2016.
[119] Info-communication Media Development Authority. "Multi-Tier Cloud Security Certified Cloud Services." February 2018.

These standards serve as a baseline for CSPs to better understand the needs of banks and provide services that comply with the regulations in the financial industry.

The United Kingdom and the European Union are also prime examples of jurisdictions that have put forward regulations on cloud adoption for financial institutions. In 2016, the Financial Conduct Authority (FCA) set out principles for cloud adoption by banks and were given the flexibility to comply based on their firm's risk preferences.[120] The Bank of England (BoE) published a framework in 2014 that focused on cybersecurity called the CBEST framework.[121] It was designed to help regulators, infrastructure providers, and financial institutions improve their understanding of cyber-attacks that could undermine financial stability in the UK, though it does not explicitly address cloud.[122] Led by the BoE, the framework involves a four-phase intelligence-led penetration test that was criticized by the Financial Stability Institute for lacking the necessary "experienced cyber/information security professionals."[123] There are also concerns that the penetration test could disrupt the real-life systems.[124] In the European Union, the European Banking Authority (EBA) published outsourcing guidance in 2006, known as the Committee of European Banking Supervisors guidelines on outsourcing (CEBS guidelines). During 2017, EBA published a final report for Recommendations on Outsourcing to CSPs based on the CEBS guidelines. These recommendations provide banks with prescriptive guidance on materiality assessments, supervisory communications, auditing, the protection and security of data and systems, chain outsourcing, and contingency plans and exit strategies.[125] The Guidelines on Information and Communication Technology (ICT) Risk Assessment focuses more on the methodologies and procedures for the assessments and specifically recognizes CSPs as a service provider. Senior management are given the flexibility to make their own decisions on whether or not to outsource services based on their risk assessments.[126]

These four jurisdictions use a combination of prescriptive, principles-based and risk-oriented guidelines, regulations and penetration tests to help direct safe and secure cloud adoption by financial institutions. While the UK's penetration test helps identify vulnerabilities in the financial system, it could be amended to specifically test the outsourcing relationship between CSPs and banks. Additionally, US regulators can look to any of these jurisdictions to build domestic guidelines on cloud adoption within the financial sector and more adequately address cloud risks in their existing frameworks. See Appendix for a detailed summary on the various cybersecurity regulations in Hong Kong, Singapore, the United Kingdom and the EU.

Observations and Analysis

- Regulators and government bodies have created just a few key documents related to cybersecurity. These documents are generally risk-oriented and technology-neutral, leaving specific security measures up to the discretion of the banks.

[120] W. Kuan Hon, Christopher Millard. "Banking in the cloud part 2 – regulation of cloud as 'outsourcing'." April 2018.
[121] Bank of England. "Financial sector continuity." April 2018.
[122] CREST. "Bank of England works with CREST to deliver cyber-security framework." June 2014.
[123] Bank of International Settlements. "Regulatory approaches to enhance banks' cyber-security frameworks." August 2017.
[124] Tom Reeve. "What's wrong with CBEST?" July 2015.
[125] EBA. "Final report: Recommendations on cloud outsourcing to cloud service providers." December 2017.
[126] EBA. "Final report: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)" May 2017.

- The OCC Bulletin expanded the scope of third-party risk assessment to include all of a bank's third-party relationships. This broad definition means that CSPs are implicitly covered by OCC guidance, but there is no cloud-specific language.
- Recently, organizations have been updating their frameworks to contain language that is specific to cloud adoption. However, these additions may not be sufficient to capture the risks that cloud adoption poses. The level to which cloud security is emphasized also varies between regulatory bodies, indicating the need for a more unified message.
- With exception to the FFIEC, many existing cybersecurity frameworks ignore concentration risk. This omission is especially dangerous given the lack of diversity among cloud providers. It is important for regulators to acknowledge that the cloud is a significant market infrastructure with low substitutability and amend existing frameworks accordingly.
- Current cyber exercises for the financial sector do not incorporate the cloud. Cloud related exercises could help yield development of industry best practices. Data backup solutions, such as Sheltered Harbor, could also address cloud use. Financial institutions could consider the same methodology of data storage when leveraging the cloud by implementing uniform formatting and data encryption.
- Currently, the information sharing platforms are not bridging the gap between the financial sector and the tech-oriented CSPs.
- Regulators outside the US have made more progress when it comes to guiding cloud adoption and management of financial institutions. As financial institutions move more of their business functions towards the cloud, industry-wide regulation of the third-party vendor risks of CSPs will become necessary to increase the resilience of financial sector and promote financial stability.

Part 4: Final Recommendations

As the cloud continues to evolve and financial institutions incorporate cloud adoption into their long-term corporate strategies, it is prudent that there be a combination of industry best practices and principles-based regulations to guide this developing technological landscape. Based on conversations with professionals in banks, consulting, insurance, clearing houses, and regulatory bodies, we have concluded that stringent regulations over the cloud would be counterproductive in an environment that is rapidly changing and it could disincentivize innovation within the financial industry. Instead, we propose a set of recommendations for banks, cloud service providers, regulators, and government that will accommodate dynamic and adaptive risk profiles and provide guidance on how to prudently adopt the cloud while mitigating threats from cyber risk and to financial stability as a whole.

Banks

Diversify Cloud Service Providers

One of the most pressing questions when it comes to the future of the cloud and finance is how banks can protect themselves from cloud outages and breaches and still serve its clients? Currently, banks are leveraging mostly AWS and Azure with smaller CSPs accounting for a much lower percentage of financial

services. Because banks have their cloud services concentrated in predominately two large providers, it poses valid concerns of concentration risk. It is critical that banks diversify their CSP partners. At the firm level, banks can leverage multiple CSPs and distribute their function to multiple facilities within a single CSP, and on the industry level, G-SIBs must ensure that they are not all housed under the same CSP, specifically in regards to their critical functions.

Anticipate Cloud Outages

We recommend banks make recovery and business continuity plans for probable cloud disruption or outage. Depending on the event, cloud-based business functionalities should be considered to port to another CSP or another server within the same CSP or even return to banks' own data center. Since portability of banking functions is critical for business continuity plans, banks could standardize a format of data so there is minimal friction in shifting operations when a significant cloud incident happens.

Classify and Map Bank Functions

Currently, there is no industry consensus on what is safe to host on the public cloud. Banks are deploying a variety of private, public and hybrid cloud strategies with little information sharing or transparency amongst their industry peers. We recommend that banks classify their bank functions as to what is core vs. non-core to assist in the cloud migration process. While some finance professionals agree that banks should be responsible for choosing what to deploy to the cloud, dependent on their risk appetite, it is prudent that banks identify which functions could pose systemic threats to the financial system if impacted. Classifying these functions internally and developing an industry consensus could help shield the financial system from cloud events.

Cloud Service Providers

Establish Cloud-ISAC

We recommend that the CSPs establish an information sharing platform for their industry to strengthen the overall public cloud environment. Through the CSP-ISAC, cloud service providers will be able to collaborate on critical security threats facing public cloud infrastructure while receiving antitrust protections from the Department of Justice. Furthermore, the organization could promote standardized processes to map risk assessments across client groups, improve "cyber hygiene" practices, and reduce concentration risk at both the firm and industry levels. We believe that CSPs may be able to leverage existing institutions such as the IT-ISAC to minimize costs and expedite the process.

Establish Information Sharing Agreement with FS-ISAC

With the establishment of a CSP-ISAC we recommend that the members arrange an information sharing agreement with the FS-ISAC as well as other industry dependencies, such as the energy and telecommunications sectors. Financial institutions need to know what vulnerabilities and threats their business may be exposed to when using cloud services. This includes increasing visibility of supply chain and multi-tenant risks that can be unique to the cloud environment. Establishing an agreement between

sectors will assist in creating high level situational awareness among participants regarding the security vulnerabilities and systemic triggers that exist between industries.

Financial Regulators

Implement Industry-Wide Stress Tests

Based on the observation and analysis that there is no industry-wide third-party stress test, we recommend that financial regulators should implement a uniform, principle-based stress test among financial institutions on the risks associated with cloud providers and cloud service. The stress testing should focus on the ability of financial institutions to recover and continue their critical functions as well as operations when a cloud event happens, for example there could be cloud outage scenarios of 30%, 50%, 70%, and 100%. As we suggest that financial institutions are responsible to determine how to utilize cloud services based on their risk appetites, the industry-wide stress test can serve as proof to the regulators that financial institutions can manage the risks associated with cloud adoption and keep the financial system stable. We also recommend that financial sector and public sector coordinate to identify test metrics and design the key indicators and scenarios. Regulator-led stress test on CSPs is also a possible direction in the future to strengthen the relationship between regulators and CSPs and allow regulators to better understand cloud services.

Develop a Standardized Cyber Risk Framework

We believe it is prudent for regulators to promote a standardized supervisory cyber risk management framework for third-party cloud adoption among financial institutions as standard cyber risk frameworks are not sufficient. Banks switching from traditional IT infrastructure to the third-party cloud providers must alter their cyber risk management frameworks to account for the additional operational risk. Fortunately, NIST has already developed a cloud consumer's risk management process that could be used by regulators in their guidance. With this framework, banks will have a strong reference point to craft their own unique risk management frameworks that account for their individual risk appetites.

Cloud Provider Supplemental Guidance

Regulators could develop a checklist of essential clauses to include in SLAs between financial institutions and CSPs. The document could follow the structure of OCC's *Supplemental Examination Procedures for Risk Management of Third-Party Relationships*. The proposed guidance would provide procedures for examiners to access the risk posed to banks by CSPs by evaluating five categories of risk 1) Credit, 2) Operational, 3) Compliance 4) Strategic 5) Reputation under four different metrics: 1) Quality of risk, 2) Quality of risk management, 3) Aggregate level of risk, 4) Direction of risk. Although the OCC third-party guidance is already being applied to CSPs, due to their size, complexity, and growing prominence in the financial sector, we believe that it is prudent to have guidance that is specific to the cloud that can incorporate unique threats such as concentration risk. Furthermore, the proposed document could include the focal areas highlighted by the EBA's guidance for cloud service providers which includes the security of data and systems, the location of data and data processing, access and audit rights, chain outsourcing, and contingency plans and exit strategies.

Reduce Regulatory Fragmentation

Regulatory bodies should present a unified message to financial institutions about how to reduce systemic risk from cloud adoption. An important step toward achieving this goal is to develop a common lexicon that is shared between regulators, financial institutions and CSPs to avoid confusion and mitigate compliance risk. Regulatory bodies should also issue rulemaking in coordination (such as with the FFIEC) to ensure supervision is uniform and standardized across financial institutions, and to reduce the burden of over regulation on banks. Finally, international organizations should collaborate on global standards and efforts to harmonize regulation, which will require trust and close dialogue between regulators, supervisors and financial institutions. We recommend standardizing cybersecurity guidelines be a priority for the G-20's FSB.

Government Agencies

Consider Designating the Cloud as Critical Infrastructure

In order to mitigate systemic risk posed by financial institutions' adoption of cloud computing, the Department of Homeland Security should consider designating CSPs as critical infrastructure under President Obama's Executive Order 13636, Section 9. The term critical infrastructure refers to systems so vital to the US that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety. Based on our assessment of cloud adoption trends, we believe CSPs qualify as critical infrastructure to the US.

Consider designating CSPs as SIFMUs by the FSOC

Cloud adoption is a general trend that financial institutions are following actively. Thus, as CSPs demonstrate to the financial industry that they can provide cloud services efficiently and robustly, banks might consider outsourcing more of their critical functions to the cloud. If this is the case, the Financial Stability Oversight Council (FSOC), authorized by the Dodd-Frank Act, should consider designating CSPs as Systemically Important Financial Market Utility (SIFMU). The designation of CSPs as SIFMUs will promote robust risk management, and safety and soundness of the cloud service industry. It will also instill more confidence in the cloud service industry as well as the financial institutions who are utilizing the cloud.

Create Joint Exercises for Financial Institutions, CSPs, and Regulators

Current exercises are very helpful in finding and addressing cybersecurity vulnerabilities in the financial system to promote financial stability. However, they do not address the risks associated with cloud adoption of financial institutions. While cloud-related risks are also important to the financial industry, we recommend regulators to improve the current existing cyber exercises by bring in CSPs as one of the key stakeholders and add cloud scenarios based on the risks associated with cloud adoption of the financial industry.

Conclusion

The cloud is an innovative and changing technological force that is quickly penetrating and changing industries around the world. The financial sector has been presented with a scalable, flexible and cost-effective solution to enhance their client experiences and improve the efficiency of business operations. Despite apparent third-party vendor risks associated with cloud adoption, banks are not likely to cease their migration to the cloud.

We agree that cloud-related cyber incidents or outages could pose serious systemic threats to the financial system however, there are various mitigation strategies that can be deployed to foster financial stability. It is clear the cloud will become an irreplaceable infrastructure for banks. To prepare for this future-state, it is critical that financial institutions, regulators, CSPs and government collaborate closely to protect and enhance the security of what is entrusted to the cloud.

Through our research and interviews with industry professionals across sectors, we are confident that financial stability can be secured with best practices and risk-oriented solutions that connect financial institutions, cloud service providers, governments and regulatory bodies.

APPENDIX 1: Cybersecurity Regulations of Various Jurisdictions

Jurisdiction	Regulation/ Guidance/ Recommendations	Year	Regulatory Body	Applicable Body	Voluntary/ Mandatory	Addresses Third-party risk	Addresses cloud outsourcing
Hong Kong	Supervisory Policy Manual on Outsourcing (SA-2)	2001	HKMA	Authorized Institutions	Mandatory	Yes	Yes
	General Principles for Technology Risk Management (TM-G-1)	2003	HKMA	Authorized Institutions	Mandatory	Yes	No
	Cybersecurity Fortification Initiative (CFI)	2016	HKMA	Authorized Institutions	Voluntary	Yes	No
Singapore	Technology Risk Management Guidelines	2013	MAS	Financial Institutions	Mandatory	Yes	Yes
	Outsourcing Guidelines	2016	MAS	Financial Institutions	Mandatory	Yes	Yes
	Cloud Implementation Guide 1.1 (ABS Guide)	2016	The Association of Banks in Singapore (ABS)	Banks	Voluntary	Yes	Yes
	Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584	2016	Singapore Standard Council	Cloud Providers	Voluntary	Yes	Yes
United Kingdom	CBEST Framework & Penetration Test	2014	BoE and HM Treasury	Financial Service Sector	Voluntary	Yes	No
	Guidance for firms outsourcing to the "cloud" and other third-party IT services	2016	Financial Conduct Authority	All Firms Authorized under FSMA	Mandatory	Yes	Yes
European Union	Committee of European Banking Supervisors Guidelines on Outsourcing	2006	CEBS	Licensed Credit Institutions	Mandatory	Yes	No
	Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)	2017	EBA	Banks	Mandatory	Yes	Yes
	Recommendations on outsourcing to cloud service providers	2017	EBA	Banks	Mandatory	Yes	Yes

Bibliography

9 to 5 Mac. “Apple and Cisco Partner with Insurance Companies to Offer Discounts for Cyber-crime Insurance.” 2018.

Arcitura. “Cloud Deployment Models.” Accessed 2018.

The Association of Banks in Singapore. “Cloud Computing Implementation Guide for the Financial Industry in Singapore.” August 2016

AWS. “AWS User Guide to Financial Services Regulations & Guidelines in Hong Kong.” November 2017.

AWS. "Capital One Case Study." January 2018.

AWS. “Financial Services Customer Success Stories," January 2018.

AWS. “Virtual Private Cloud.” Accessed 2018.

AWS. “What is cloud computing?” Accessed 2018.

Bank of England. “Financial sector continuity.” April 2018

Bank of International Settlements. “Regulatory approaches to enhance banks’ cyber-security frameworks.” August 2017.

Bluelock. “3 Things to Know About SOC 2 Compliance and Cloud Providers.” February 2018.

Bourne, J. “AWS passes $5 billion in quarterly revenue with a $20bn run rate”. February 2018

Butler, B. “How Goldman Sachs and Bank of America use the cloud and containers.” December 2015.

Capgemini. “Cloud Computing in Banking: what banks need to know when considering a move to the cloud.” 2011.

CBInsights. “Banks in FinTech: What’s Ahead in 2018.” January 2018.

The Clearing House. “Re: Enhanced Cyber Risk management Standards.” February, 2017.

Cloud Security Alliance. “Security Guidance for Critical Areas of Focus in Cloud Computing 2.1.” 2009.

Cloud Technology Partners. “How to Slay the Dragon of Cloud SLAs.” 2017.

Covington & Burling, LLP. “Federal Banking Agencies Request Comment on Enhanced Cybersecurity Standards.” October 2016.

CPMI-IOSCO. “Guidance on cyber resilience for financial market infrastructures.” June 2016.

CREST. “Bank of England works with CREST to deliver cyber-security framework.” June 2014.

The Data Center Journal. “Ten Things You Need to Know about Cybersecurity Insurance.” June 2016.

Deloitte. “Cloud Computing – What Auditors Need to Know.” 2014.

Deloitte, SIFMA. “Standing together for financial industry cyber resilience Quantum Dawn 3 after-action report.” November 2015.

DTCC. “Moving Financial Market Infrastructure to the Cloud, Realizing the Risk Reduction and Cost Efficiency Vision While Achieving Public Policy Goals.” May 2017.

EBA. “Final report: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)” May 2017.

EBA. “Final report: Recommendations on cloud outsourcing to cloud service providers.” December 2017.

ECB. “Cyber Resilience for Financial Market Infrastructure.” January 2016.

EU GDPR. “GDPR Key Changes.” Accessed 2018.

European Commission. "FinTech Action Plan: For a more competitive and innovative European financial sector." March 2018.

FBIIC. “Mission and History.” Accessed April 2018.

FFIEC. “Cybersecurity Assessment Tool.” May 2017

Finkle, J. “Bangladesh Bank hackers compromised SWIFT software, warning issued.” Reuters, April 2016.

FS-ISAC. “About.” Accessed April 2018.

FS-ISAC. “FS-ISAC announces the formation of the Financial Systemic Analysis & Resilience Center (FSARC).” October 2016.

FSB. “Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices.” October 2017.

FSSCC. “About FSSCC.” Accessed April 2018.

FSSCC. “Financial Services Sector Cybersecurity Recommendations.” January 2017.

Gartner. “Clouds Are Secure: Are You Using Them Securely?” September 2015

Gartner. “Report of Cloud Computing.” October 2017.

Gartner. “Special Report Examines the Realities and Risks of Cloud Computing.” June 2008.

Gartner. “Vendor Risk Management.” 2017.

Greenwald, G. “Glenn Greenwald: how the NSA tampers with US-made internet routers.” The Guardian, May 2014.

Gurkok, C. “Securing Cloud Computing Systems. Overview of System and Network Security: A Comprehensive Introduction.” *Network and System Security*, Synergess, 2017.

Hon, W. K. & Millard C. “Banking in the cloud: Part 2 – regulation of cloud as ‘outsourcing’.” *Computer Law & Security Review* 34.2 (2018): 337-357.

Hong Kong Monetary Authority. “Supervisory Policy Memo TM-G-1: General Principles for Technology Risk Management.” June 2003.

Hussain, W., Hussain, O. & Hussain, F. “Maintaining Trust in Cloud Computing Through SLA Monitoring.” 2014.

IBM. “Best Practices to Develop SLAs for Cloud Computing.” 2013.

IBM. “Mizuho Bank Begins API Banking on IBM Cloud to Help Drive Innovation with Partners”. June 2017.

IIF. “Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system.” September 2017.

IMF Working Paper. “Cyber Risk, Market Failures, and Financial Stability.” August 2017.

Info-communication Media Development Authority. “Multi Tier Cloud Security Certified Cloud Services.” February 2018

Iorga, M. & Karmel, A. "Managing Risk in a Cloud Ecosystem.” "*IEEE Cloud Computing*, 2.6 (2015), 51-57.

I.S. Partners. “SOC 1 and SOC 2 Reports – Do you Know the Difference?” 2018.

IsecT. “ISO/IEC 27017:2015/ ITU-T X.1631 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.” Accessed April 2018.

ISO. “ISO/IEC 27001:2013.” October 2013.

Kang, J. & Dam, R. “Journey to the Cloud.” June 2017

Lloyd’s & AIR Worldwide. “Cloud Down: Impacts on the US Economy”. January 2018.

Marsh and McLennan. “The Role of Cybersecurity in Risk Management.” 2016.

McKinsey & Company. "Data Sharing and Open Banking." September 2017.

McKinsey & Company. “Making a secure transition to the public cloud.” 2017

Microsoft. “Earnings Release FY2017 Q4.” July 2017.

Microsoft. “Navigating your way to the cloud – Microsoft’s response to the MAS Outsourcing Guidelines and the ABS Cloud Implementation Guide.” November 2016.

Nash, K.S. “J.P. Morgan Set to Run First Apps in Public Cloud.” *The Wall Street Journal*, March 2017.

Microsoft Azure. “What are public, private and hybrid cloud?” Accessed February 2018.

Microsoft News Center. “Bank of America chooses the Microsoft Cloud to support digital transformation.” October 2017.

Monetary Authority of Singapore. “Guidelines on Outsourcing.” July 2016.

NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0.” February 2014.

NIST. “Managing Risk in a Cloud Ecosystem.” December 2015.

NIST. “NIST Publishes Draft Cloud Computing Security Document for Comment.” June 2013.

OCC. “Bulletin 2013-29: Third-Party Relationships.” October 2013.

OCC. “Fiscal Year 2018 Bank Supervision Operating Plan.” September 2017.

OCC, FRB & FDIC. “Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards.” October 2016.

Office of Financial Research. “Cybersecurity and Financial Stability: Risks and Resilience.” February 2017.

Pelnekar, C. “Planning for and Implementing ISO 27001.” *ISACA Journal* 4 (2011).

PwC. “Financial Services Technology 2020 and Beyond: Embracing disruption.” 2016.

PwC. “Insurance 2020 and beyond: Reaping the dividends of cyber resilience.” 2015.

PwC. “System and Organization Controls Reporting.”

Quartz. “Amazon is invading finance without really trying”. November 2017.

Rathod, L. “European Banking Authority: New Outsourcing Guidelines Seek to Clear the Path to the Cloud for the Finance Industry.” *Diligent.* 2018.

RedLock CSI Team. “The Cryptojacking Epidemic.” February 2018.

Reeve, T. “What’s wrong with CBEST?” July 2015.

SANS. “Proposal for standard Cloud Computing Security SLAs – Key Metrics for Safeguarding Confidential Data in the Cloud.” 2015.

SIFMA. “Fact Sheet: Quantum Dawn IV.” November 2017.

Silicon. “HSBC Embraces Google Cloud For Big Data Analytics And Money Laundering Detection.” May 2017.

Skytap. “Skytap Announces $45 million Series E Led by Goldman Sachs”. August 2017.

Symmetry. “Virtual Private Cloud vs Private Cloud: What’s the difference?” Accessed 2018.

Third Certainty. “Deloitte-Zurich form Partnership to Offer Cyber Risk Services.” 2018.

ThousandEyes. "Amazon AWS Outage a Lesson in Managing Cloud First Risks." March 2018.

Wall Street Journal. "Next Up for Amazon: Checking Accounts." March 2018.

Wall Street Journal. “Why Amazon and Google Haven’t Attacked Banks.” April 2018.

Wired. “Service Level Agreements in the Cloud.” 2011.

Woodruff, Sawyer, and Company. “Cyber Insurance 101: Cloud Computing and Liability.” August 2014.